Б.Г. Койбаев, З.Т. Золоева

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИСТСКИМ ПРОЯВЛЕНИЯМ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

Владикавказ 2021

МИНИСТЕРСТВО РЕСПУБЛИКИ
СЕВЕРНАЯ ОСЕТИЯ – АЛАНИЯ ПО НАЦИОНАЛЬНОЙ
ПОЛИТИКЕ И ВНЕШНИМ СВЯЗЯМ

Б.Г. Койбаев, З.Т. Золоева

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИСТСКИМ ПРОЯВЛЕНИЯМ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

Владикавказ 2021

ББК 66.3(2Рос)3
К 55

Исполнено в рамках реализации Государственной программы Республики Северная Осетия – Алания «Развитие межнациональных отношений в Республике Северная Осетия – Алания» на 2019-2025 годы, подпрограмма 2 «Профилактика экстремизма на национальной религиозной почве и идеологии терроризма в Республике Северная Осетия – Алания».

При консультативной поддержке заместителя Министра РСО-Алания по национальной политике и внешним связям ***В.В. Леся***

Рецензенты:
доктор политических наук, профессор ***Ю.В. Усова,***
доктор исторических наук, профессор ***А.К. Дудайти***

Койбаев Б.Г., Золоева З.Т. Актуальные проблемы противодействия экстремистским проявлениям в условиях развития цифровизации: монография / Б.Г. Койбаев, З.Т. Золоева; Миннац РСО-Алания. – Владикавказ: ИПЦ ИП Цопанова А.Ю., 2021. – 192 с.

ISBN 978-5-00081406-2

В монографии рассматриваются теоретические и практические подходы к актуальным проблемам противодействия экстремистским проявлениям в условиях развития современной цифровизации. На примере Республики Северная Осетия – Алания показана профилактика борьбы с проявлениями экстремизма в сети Интернет.

Книга адресована исследователям и преподавателям образовательных учреждений, государственным и муниципальным служащим, работникам правоохранительных органов, а также тем, кто непосредственно занят проблемами противодействия экстремистской деятельности.

ББК 66.3(2Рос)3К

ISBN 978-5-00081406-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие процессов цифровизации знаменует новый этап в судьбе человечества. На этом этапе роль техники безмерно возрастает, а человек утрачивает свою былую роль главного инициатора и двигателя прогресса. Новый социо-технологический уклад жизни лишает человека самой возможности что-либо решать без инновационных технологий, и даже само их появление выходит у него из-под контроля.

Очевидно, что эти процессы подводят человечество к определенной черте, за которой уже прорисовывается принципиально новый мир, основания которого требуют глубокого осмысления. В своей основе цифровизация прежде всего предполагает трансформацию значимой информации в цифровую форму для обеспечения ее эффективного использования в разных областях человеческой деятельности и формирования новых коммуникативных и познавательных возможностей.

Расширяя же эти возможности, цифровизация сама уже создает новые среды обитания человека – цифровые, технологические, отличные от реальности, но претендующие на ее более совершенную замену. Развернувшаяся цифровизация формирует новый тип культуры современного общества – цифровую культуру.

Важно отметить, что это один из многообразия существующих типов культуры и, будучи явлением временным, т.е. вызванным изменчивыми условиями эпохи, он должен проявить свой позитивный потенциал в нахождении единства с цельной систе-

мой национальной культуры, реализуя в себе ее базовые ценности и обогащая ее своими возможностями.

Сотворив цифровое пространство своей жизнедеятельности, человек стал носителем его неотъемлемых свойств, которые находят воплощение в образе мыслей, действий, физическом и психологическом состоянии людей. Социальные проявления погружения человека в цифровой мир становятся главными источниками осмысления характера формирующейся цифровой культуры.

Анализ социальных проявлений цифровой культуры позволил сформулировать ее следующие характеристики: технологическая мощь, привлекающая скоростями получения и передачи информации, упрощением форм социальной и личной жизни человека; программируемость человеческого поведения, его зависимость от цифровых кодов; формализация и фрагментация коммуникационных процессов, ослабление их этического содержания, замкнутость человека в проблематике личного комфорта; преобладание клипового мышления, визуального восприятия мира; технологизм, проникающий и в сферу человеческих отношений, углубляющийся разрыв с традициями гуманитарной культуры; появление особого языка общения.

Цифровая модернизация в нашей стране носит «неорганический» характер, что определяется отсутствием четко сформированной общественной потребности, социального запроса на цифровые изменения. Модернизацию такого типа стимулирует государство, комплекс общеобязательных для исполнения нормативно-правовых и иных регламентирующих актов, исходящих из специализированных административных структур и часто не находящих понимания в широких слоях субъектов общества.

Сегодня все более очевидна нехватка ценностно-целевой составляющей процесса цифровой модернизации общества. Актуальным в современных условиях становится определение соотношения цифровых реформ с ценностями общечеловеческой

культуры, проблемами безопасности, противодействием экстремистских проявлений[1].

Президент России Владимир Путин на заседании Совета по правам человека заявил о том, что необходимо бороться с экстремизмом в социальных сетях. Глава государства обратил внимание на то, что соцсети «все чаще и чаще используются именно для экстремистской деятельности», и в этой связи государство должно противостоять этому явлению.[2]

Основная опасность (и, соответственно, актуальность исследуемой проблемной области) заключается в гносеологическом вакууме относительно феномена информационного экстремизма. Отсутствие объективных, научно обоснованных данных о причинах, характере проявления, социальных последствиях применительно к основным социальным институтам приводит к серьезному научному и управленческому кризису. В результате правоохранительные органы, государственные управленческие структуры не могут адекватно реагировать на инновационные угрозы начала XXI в., а информационные экстремисты обладают стратегической инициативой.[3]

В обществе XXI в. информационный экстремизм чаще всего реализуется посредством глобальной сети Интернет, различных ее социоструктурных элементов. Интернет – это и всеобъемлющий накопитель различной информации, и источник новых решений, основанных на уже накопленной информации.[4]

---

1 Багаева А.А. Проблемы государственной политики по противодействию экстремизму и терроризму в СМИ и Интернет-пространстве // Право и государство, общество и личность: история, теория, практика: Сборник научных статей участников VII Всероссийской научно-практической конференции с международным участием. 2018. С. 32.

[2] Совет по правам человека / [Электронный ресурс] // Режим доступа http://molgvardia.ru/nextday/2016/12/09/89799

[3] Мозговой В.Э. Информационный экстремизм в условиях социо-коммуникативных трансформаций российского общества: Дисс. ... к. с. н. Краснодар, 2015. С. 3.

[4] Беляев Д.А. Интернет как основа информационного общества / [Электронный ресурс] // Режим доступа: http://www.gosbook.ru/system/files/documents/2011/09/01/k-1-1-11-informatizacija.pdf.

В пространстве глобальной сети информационный экстремизм серьезным образом диверсифицируется, распространяя свое влияние на социальные сети, форумы, чаты, блоги, сайты различной тематической направленности.

ГЛАВА 1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

1.1. Теоретико-методологические подходы к проблеме цифрового общества

Современный этап развития общества характеризуется беспрецедентными достижениями в области информационно-коммуникационных технологий (ИКТ), которые изменили привычный уклад жизни в различных странах независимо от уровня их экономического развития. Внедрение Интернета и устройств нового поколения, которые могут общаться через Интернет, значительно повлияло как на повседневную жизнь людей, так и на их способ ведения бизнеса. Все сферы жизни общества были подвергнуты этим изменениям, а их последствия имеют долгосрочный и трудно прогнозируемый характер как для общества, так и для экономики. Так, благодаря достижениям новых информационно-коммуникационных технологий люди могут связаться друг с другом практически мгновенно, находясь в разных точках земного шара. Можем осуществлять трудовую деятельность не выходя из дома, получать образование, медицинскую помощь, различные государственные услуги, что позволило повысить качество жизни людей.

С экономической точки зрения эти технологические достижения повлияли на нашу жизнь двумя фундаментальными способами. Во-первых, предоставляя доступ к огромным объемам информации. Во-вторых, снижая операционные издержки, эти технологии способствовали повышению экономической эффективности. Например, во многих странах клиент может оплачивать счета за коммунальные и иные услуги, а также товары при помощи кредитной карты – онлайн, что позволяет экономить время. Кроме того, возможность осуществления платежей в любое время суток повышает удобство для клиента. Приведенные изменения связаны с развитием информационного общества.

Термин «информационное общество» был предложен для обозначения постиндустриального общества, в котором инфор-

мация играет ключевую роль. За последние полвека было предпринято несколько попыток концептуализировать основные характеристики информационного общества, в каком направлении, по мнению некоторых мыслителей, будет развиваться общество. В различных определениях, которые были предложены на протяжении многих лет, существует пять основных характеристик информационного общества: технологическая, экономическая, социологическая, пространственная и культурная.

Профессор Ю. Хаяши считается первым, кто использовал термин «информационное общество». Теория информационного общества в дальнейшем была детально разработана в трудах таких авторов, как М. Порат, Й. Масуда, Т. Стоуньер, Р. Катц, М. Маклюэн и др. Согласно Хаяши, информационное общество было определено как общество, в котором процесс компьютеризации предоставил людям доступ к достоверной информации, избавил их от рутинной работы и обеспечил высокий уровень автоматизации. Производство также меняется – его продукт становится более информационным в области инноваций, дизайна и маркетинга, возрастает его ценность. Производство информационных товаров (а не материальных) становится основой экономического роста.[5]

В 70-е годы эта концепция стала популярной в США и Европе и превратилась в универсальную идеологию. Американский социолог Д. Белл, автор постиндустриального общества, представил версию конвергенции постиндустриального и информационного общества.[6] Согласно исследованиям Белла, информационное общество – это новое название постиндустриального общества, подчеркивающее не его положение (в контексте социального развития после индустриального общества), а основу для определения его социальной структуры, т. е. информация.

Создание информационного общества было одной из стратегических целей многих стран. Одной из первых стран, где был

[5] Masuda Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983.

[6] Bell D. The Social Framework of the Information Society. Oxford, 1980. На рус. яз.: Белл Д. Социальные рамки информационного общества / Сокращ. перев. Ю.В. Никуличева // Новая технократическая волна на Западе / Под ред. П.С. Гуревича. М., 1988.

осуществлен переход к информационному обществу, можно назвать Японию и США.

Россия сегодня находится в состоянии формирования информационного общества, которое требует модернизации устройства общества, преобразования государственных и общественных институтов. На фоне процессов, происходящих на мировой арене, особую остроту приобретает проблема формирования своевременной и эффективной государственной политики в сфере информатизации и развития информационного общества.

Как справедливо отмечают С.И. Грачев, О.Н. Герасин, А.О. Колобов, М.И. Ливерко, «наряду с тем что в большинстве сфер деятельности государства происходят позитивные изменения, следует отметить, что развитие информационной организации государства переживает весьма сложный период. В результате информационная сфера, ее ресурсы, в том числе и их защищенность, отстают в развитии от других институтов современного российского общества. Данное обстоятельство негативно сказывается как на информационной организации государства, так и на состоянии информационной безопасности России, личности и всего общества в целом».[7]

Проблема разработки и реализации научно обоснованной и эффективной политики в сфере информатизации становится сегодня актуальной стратегической задачей. Являясь одним из направлений внешней и внутренней политики государства, политика в сфере информатизации охватывает своим воздействием многие важнейшие сферы общественной жизни: экономику, культуру, образование, сферу межгосударственных отношений и т.д. [8]

Базовым нормативным актом в исследуемой сфере выступает Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ, закрепляющий основные принципы регулирования отношений в

[7] Грачев С.И., Герасин О.Н., Колобов А.О., Ливерко М.И. Проблемные аспекты в информационной политике и информационной безопасности России // Вестник Нижегородского университета им. Н.И. Лобачевского. №1. 2012. С. 290.

[8] Панферова В.В. Информационная политика в современной России // Социально-гуманитарные знания. №5. 2005. С. 55.

информационной сфере, правой статус информационных ресурсов и т.д. [9]

Закон «Об информации, информационных технологиях и о защите информации» содержит статьи 15.1. «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» и 15.1-1. «Порядок ограничения доступа к информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации», введение которых, в том числе, направлено на противодействие экстремистским проявлениям в сети «Интернет».

Так, в соответствии со ст. 15.1. «В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по удалению указанной информации и по ограничению доступа к информационным ресурсам, распространяющим указанную информацию, в случае ее неудаления».[10]

[9] Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации» // Российская газета. № 165. 29.07.2006.

[10] Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации» // Российская газета. №165. 29.07.2006.

В 2006 году Правительством Российской Федерации была одобрена Концепция региональной информатизации, а летом 2007 года в качестве рамочной была утверждена Типовая программа развития и использования информационных и телекоммуникационных технологий субъекта Российской Федерации и дано поручение регионам разработать и принять у себя соответствующие программы. Следует отметить, несмотря на то, что срок действия Концепции формально завершился, затронутые в нем принципиальные вопросы отнюдь не потеряли своей значимости, а поставленные задачи оказались решены далеко не в полной мере.[11]

Важное значение для развития информационного общества в России имели такие (в настоящее время не действующие) документы, как: Закон «Об информации, информатизации и защите информации» (20 февраля 1995 года №24-ФЗ); Стратегия развития информационного общества в Российской Федерации (7 февраля 2008 года) была официально принята, устанавливающая общие стратегические ориентиры развития до 2020 года;[12] Доктрина информационной безопасности (9 сентября 2000 г); Концепция формирования в Российской Федерации электронного правительства до 2010 года (6 мая 2008 года); Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (17 ноября 2008); Концепция информатизации судов общей юрисдикции и системы Судебного департамента, утвержденная Постановлением Совета судей Российской Федерации от 11 апреля 2002 г. №75; Федеральной целевой программы «Электронная Россия (2002-2010 годы)» и др.

Однако основной объем работ по формированию в России информационного общества был осуществлен в рамках реализации государственной программы «Информационное общество (2011-2020 годы)». В тексте программы «Информационное общество (2011-2020 гг.)» отмечалось, что в России сохраняется высокий уровень цифрового неравенства регионов в использовании ин-

[11] Швецов А.Н. Государственная политика региональной информатизации: соотношение централизации и местной самостоятельности // Проблемный анализ и государственно-управленческое проектирование. №3. 2013. С. 7.

[12] Совет Безопасности утвердил Стратегию развития информационного общества // Российская газета www.rg.ru от 26 июля 2007.

формационных и телекоммуникационных технологий в домашних хозяйствах.[13] Причем основной «вклад» в расслоение регионов вносили показатели использования населением сети Интернет и доступа к ней домашних хозяйств.

Впоследствии в программу был внесен ряд изменений, и в настоящее время она называется «Государственная программа «Информационное общество»», а этапы ее реализации рассчитаны до 2024 года. В обновленной программе учтены современные тенденции, связанные с развитием цифровых технологий. Программа включает в себя 4 подпрограммы: «Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на ее основе»; «Информационная среда»; «Безопасность в информационном обществе»; «Информационное государство».

Для данного исследования интерес представляет подпрограмма «Безопасность в информационном обществе», целью которой выступает предупреждение угроз, возникающих в информационном обществе. Подпрограмма направлена на решение следующих задач: обеспечение контроля и надзора, разрешительной и регистрационной деятельности в сфере связи, информационных технологий и массовых коммуникаций; противодействие распространению идеологии терроризма, экстремизма и пропаганды насилия.

В рамках подпрограммы «Безопасность в информационном обществе» осуществляется мониторинг средств массовой информации на соответствие требованиям статьи 4 Федерального закона «О средствах массовой информации» и Федерального закона «О противодействии экстремистской деятельности»; лицензирование деятельности по изготовлению экземпляров аудиовизуальных произведений, программ для электронных вычислительных машин, баз данных и фонограмм на любых видах носителей, лицензионный контроль, долицензионные проверки соискателей лицензий; лицензирование телевизионного вещания и радиовещания, лицензионный контроль; обеспечение прав субъектов

[13] Постановление Правительства РФ от 15.04.2014 №313 (ред. от 21.10.2016) «Об утверждении государственной программы Российской Федерации «Информационное общество (2011-2020 годы)»». Опубликовано на официальном интернет-портале правовой информации // http:// pravo/gov/ru/- 25.09.2021).

персональных данных; ведение реестра операторов, осуществляющих обработку персональных данных.[14]

Доля нарушений, выразившихся в невыполнении предписаний, в общем количестве нарушений, выявленных в ходе внеплановых проверок, в том числе в сфере персональных данных, процентов (табл. 1.)

Таблица 1

	2017		2018		2019		2020
	план.	факт.	план.	факт.	план.	факт.	план
Российская Федерация	8	6	6	18,83	6	14,7	6
Северо-Кавказский федеральный округ	8	6	6	54,54	6	-	6
Республика Дагестан	8	6	6	21,42	6	8,33	6
Республика Ингушетия	8	6	6	20	6	-	6
Кабардино-Балкарская Республика	8	6	6	23,07	6	20	6
Карачаево-Черкесская Республика	8	6	6	-	6	-	6
Республика Северная Осетия – Алания	8	6	6	9,52	6	-	6
Чеченская Республика	8	6	6	50	6	-	6
Ставропольский край	8	6	6	54,54	6	-	6

*Таблица составлена на основе сведений, содержащихся в государственной программе «Информационное общество».

Доля проведенных контрольных мероприятий в сфере противодействия распространению идеологии терроризма, экстремизма и пропаганды насилия в общем количестве запланированных мероприятий, процентов (табл. 2)

[14] Постановление Правительства РФ от 15.04.2014 №313 (ред. от 31.03.2021) «Об утверждении государственной программы Российской Федерации «Информационное общество»» // Собрание законодательства РФ. 05.05.2014. №18 (часть II). Ст. 2159.

Таблица 2

	2017		2018		2019		2020	2021	2022	2023	2024
	план.	факт.	план.	факт.	план.	факт.	план	план	план	план	план
Российская Федерация	50	82	70	90	75	75	82	83	84	85	86
Северо-Кавказский федеральный округ	50	82	70	90	75	75	82	83	84	85	86
Республика Дагестан	50	82	70	90	75	75	82	83	84	85	86
Республика Ингушетия	50	82	70	90	75	75	82	83	84	85	86
Кабардино-Балкарская Республика	50	82	70	90	75	75	82	83	84	85	86
Карачаево-Черкесская Республика	50	82	70	90	75	75	82	83	84	85	86
Республика Северная Осетия – Алания	50	82	70	90	75	75	82	83	84	85	86
Чеченская Республика	50	82	70	90	75	75	82	83	84	85	86
Ставропольский край	50	82	70	90	75	75	82	83	84	85	86

*Таблица составлена на основе сведений, содержащихся в государственной программе «Информационное общество».

Доля сетевых изданий, в отношении которых осуществляется постоянный мониторинг соблюдения требований законодательства Российской Федерации в сфере средств массовой информации, в том числе на предмет выявления информации террористической и экстремистской направленности, в общем количестве активных сетевых изданий, процентов (табл. 3)

Таблица 3

	2017		2018		2019		2020	2021	2022	2023	2024
	план.	факт.	план.	факт.	план.	факт.	план	план	план	план	план
Российская Федерация	-	-	92	92	95	95	100	100	100	100	100
Северо-Кавказский федеральный округ	-	-	92	92	95	95	100	100	100	100	100
Республика Дагестан	-	-	92	92	95	95	100	100	100	100	100
Республика Ингушетия	-	-	92	92	95	95	100	100	100	100	100
Кабардино-Балкарская Республика	-	-	92	92	95	95	100	100	100	100	100
Карачаево-Черкесская Республика	-	-	92	92	95	95	100	100	100	100	100
Республика Северная Осетия – Алания	-	-	92	92	95	95	100	100	100	100	100
Чеченская Республика	-	-	92	92	95	95	100	100	100	100	100
Ставропольский край	-	-	92	92	95	95	100	100	100	100	100

*Таблица составлена на основе сведений, содержащихся в государственной программе «Информационное общество».

Доктрина информационной безопасности Российской Федерации, принятая 5 декабря 2016 года, также является важнейшим документом в исследуемой сфере. В Доктрине отмечается: «Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнета-

ния межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры».[15]

Кроме того, Доктрина выделяет в качестве одного из основных направлений обеспечения информационной безопасности «противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации». [16]

Следует отметить проводимую на федеральном уровне политику формирования нового и обновления уже действующего законодательства в сфере информатизации и повышения открытости органов государственной власти и местного самоуправления. Начиная с 2009 года, были приняты достаточно прогрессивные для нашего государства нормативно-правовые акты: Федеральный закон от 22 декабря 2008 г. №262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» и Федеральный закон от 9 февраля 2009 г. №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Данные законодательные акты, являясь новеллами отечественного законодательства, выступают в качестве одной из основ электронного государства, к построению которого стремится Россия. Первый законодательный акт предусматривает возможность получения информации о деятельности судов, в том числе через сеть Интернет. К сожалению, Закон не содержит обязанно-

[15] П. 13 Указа Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. №50. Ст. 7074.

[16] П. 23 Указа Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. №50. Ст. 7074.

сти судебных органов иметь официальные сайты, а лишь предусматривает возможность использования сети Интернет, в которой они могут создаваться.[17]

Особое место в системе политико-правовых документов, направленных на развитие информационного общества, имеет Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, призванная обеспечить реализацию национальных интересов РФ, среди которых наряду с развитием человеческого капитала и обеспечением безопасности выделяется формирование в стране цифровой экономики и необходимость повышения эффективности государственного управления.[18]

Современные тенденции развития информационного общества во многих странах мира связаны с развитием процесса цифровизации. В этой связи в Российской Федерации была принята Государственная программа «Цифровая экономика Российской Федерации», утвержденная Распоряжением Правительства Российской Федерации от 28 июля 2017 г. №1632-р.[19] Принятие данной программы способствовало масштабным изменениям в системе российского законодательства как на федеральном, так и на региональном уровне.

Таким образом, можно заключить, что в России на протяжении многих лет реализуется политика в сфере информатизации, однако реализация ее на практике сталкивается с рядом проблем технологического, экономического, а иногда и правового характера. Как известно, переход к информационному обществу является глобальной тенденцией, в связи с чем роль целенаправленной общегосударственной политики в исследуемой сфере возрастает.

---

[17] Ст. 10 Федерального закона от 22 декабря 2008 г. №262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Российская газета. Документы. От 26 декабря 2008 г.

[18] Указ Президента РФ от 09.05.2017 №203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ. 15.05.2017. №20. Ст. 2901.

[19] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 №7) / [Электронный ресурс] // Режим доступа: http://government.ru/info/35568/

В этой связи видится необходимым постоянное совершенствование политических и правовых документов, а также заимствование зарубежного опыта в сфере информатизации и развития информационного общества. В условиях непрерывного процесса развития информационно-коммуникационных технологий обостряется проблема обеспечения информационной безопасности и противодействия проявлениям экстремизма.

1.2. Цифровизация как тенденция развития современного общества

Процесс формирования в России демократического правового государства находится в дихотомической связи с постоянно развивающимся и эволюционирующим информационным обществом. Как известно, развитие информационного общества в настоящее время связано с реализацией проектов развития цифровой экономики. В связи с чем в юридической литературе все чаще встречается термин «цифровизация». Мы полностью разделяем мнение В.Д. Зорькина о том, что в условиях развития цифровой реальности «прежнее нормативно-правовое регулирование различных сфер социальной жизни нуждается в существенной модернизации».[20]

Цифровизация – это новая тенденция развития современного общества. Её рассматривают в качестве ключевого тренда, характерного для различных отраслей хозяйства, секторов экономики и иных сфер. С ее развитием связываются ожидания, направленные на повышение эффективности и облегчение функционирования как государственных органов, так и предприятий и иных акторов. Стратегии цифровой трансформации часто направлены на трансформацию (изменение) продукции, процессов, организацию деятельности (управления) на основе применения инновационных технологий.[21]

---

[20] Зорькин В.Д. Право в цифровом мире: Размышление на полях Петербургского международного юридического форума // Российская газета. Столичный выпуск. №115.

[21] Matt C. et al. Digital Transformation Strategies // Business and Information Systems Engineering. 2015. Vol. 57. №5. P. 339-343.

Под цифровизацией в узком смысле понимается преобразование информации в цифровую форму, которое в большинстве случаев ведет к снижению издержек, появлению новых возможностей и т.д. Большое число конкретных преобразований информации в цифровую форму приводит к таким существенным положительным последствиям, которые обусловливают применение термина цифровизации в широком смысле.[22]

В современных условиях цифровая трансформация является одним из основных бизнес-приоритетов. Так как с каждым годом увеличивается количество продуктов и услуг, предлагаемых клиентам по цифровым каналам для их удобства, в то время как традиционные способы продаж стремительно сокращаются.

Автоматизация позволяет повысить эффективность как государственного управления, так и управления компанией. Сбор, хранение и обработка данных помогают генерировать аналитическую информацию для принятия решений и направлять в правильном курсе для ее процветания. Кроме того, цифровизация несет с собой ряд преимуществ и для удовлетворения потребностей граждан и бизнеса, в том числе способствуя облегчению получения государственных услуг в электронной форме.

Цифровые технологии вносят важные метаморфозы в жизнь граждан. Так, они позволяют расширить возможности граждан в сфере реализации важнейшего конституционного права – права на доступ к информации. И в то же время реализация данного права налагает на государство обязанность по его обеспечению. В связи с чем деятельность государства также становится немыслимой без применения цифровых технологий. Зарубежные исследователи зачастую используют термины «цифровое государство», «цифровое государственное управление».

Так, например, все европейские страны приняли стратегии, направленные на содействие цифровизации государственного сектора. Девять государств – членов ЕС приняли законы, стимулирующие развитие ИКТ. С ростом важности и популярности цифровых государственных услуг среди граждан и предприя-

[22] Халин В.Г., Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. 2018. №10. С. 47.

тий национальные правительства начали реорганизацию своих структур управления, выделив одно ответственное министерство или орган по вопросам цифрового управления. Некоторые страны больше внимания уделяют предоставлению цифровых общественных услуг на местном уровне, что делает важным приоритетом цифровизацию при помощи небольших офисов. Предоставление государственных услуг, ориентированных на граждан и бизнес, является постоянно растущим приоритетом во всех государствах – членах ЕС.[23]

Применение цифровых технологий в деятельности органов государственной власти позволяет повысить прозрачность их деятельности, сделать их более открытыми и в то же время доступными для граждан. В этих условиях право на доступ к информации приобретает новое содержание, связанное с возможностью доступа к информации посредством цифровых технологий и обязанностью органов государственной власти обеспечить доступ к такой информации.[24]

По нашему мнению, информационная открытость органов государственной власти позволяет обеспечить процесс наиболее эффективного взаимодействия государства, граждан и институтов гражданского общества. Обеспечение открытости в деятельности органов государственной власти повышает доверие к власти, способствует повышению доступности, снижению административных барьеров. Кроме того, открытость органов государственной власти помогает снизить коррупционные риски и прямым образом влияет на повышение качества государственного управления.

Цифровизация повлияла на развитие инструментов электронной демократии. Однако, как справедливо отмечает Э.В. Талапина, имеются серьезные опасения использования Интернета и социальных сетей.[25]

---

[23] How were the governments in Europe digitalised in last 10 years? https://ec.europa.eu/isa2/news/how-were-governments-europe-digitalised-last-10-years-read-our-new-report_en

[24] Золоева З.Т. Некоторые проблемы реализации права на доступ к информации (на материалах РСО-Алания) (Часть 1) // Информационные ресурсы России. 2017. №1 (155). С. 40-45.

[25] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. №2. 2018. С. 5-17.

Должностные лица и органы государства имеют аккаунты в социальных сетях, однако их статус не регламентирован. В связи с чем высказываются мнения о необходимости ведения цифрового реестра, фиксирующего официальные страницы государственных органов и должностных лиц в социальных сетях.[26]

Одной из важных проблем, возникающих в связи с использованием цифровых технологий, выступает обеспечение информационной безопасности.[27]

Так, 26 июля 2017 года был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» №187-ФЗ, вступивший в силу с 1 января 2018 года. Законом закреплена необходимость формирования Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Кроме того, Закон установил необходимость создания Национального координационного центра по компьютерным инцидентам. С целью учета значимых объектов критической информационной инфраструктуры Федеральной службой безопасности Российской Федерации[28] осуществляется ведение Реестра значимых объектов критической информационной инфраструктуры.

По нашему мнению, в современных условиях проблематика организации государственного управления с области обеспечения информационной безопасности носит первостепенный характер. Так как эффективность осуществления мероприятий по обеспечению информационной безопасности прямым образом зависит от организации системы управления.

---

[26] Парфенчик А.А. Использование социальных сетей в государственном управлении // Вопросы государственного и муниципального управления. 2017. №2. С. 186-200.

[27] Золоева З.Т. Некоторые проблемы реализации права на доступ к информации (на материалах РСО-Алания) (Часть 2) // Информационные ресурсы России. 2017. №2 (156). С. 20-23.

[28] Указ Президента РФ от 22.12.2017 №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства РФ. 25.12.2017. №52 (Часть I). Ст. 8112.

Представляется важным также отметить и необходимость совершенствования механизмов обеспечения информационной безопасности личности.[29]

Так как при использовании цифровых технологий (например, больших данных) создается угроза нарушения конфиденциальности данных. Таким образом, возникает противоречие между необходимостью обеспечения открытости органов государственной власти и защитой прав физических лиц. Все это свидетельствует о необходимости дальнейшего развития административно-правовых основ применения цифровых технологий в государственном управлении.

Важно также отметить, что в современных условиях информационные технологии широко используются экстремистскими и террористическими организациями в своей деятельности, что является еще одним из направлений обеспечения информационной безопасности (об этом более подробно в главе 2).

Процесс развития информационного общества является непрерывным, он будет постоянно эволюционировать, что непременно будет требовать реакции со стороны законодателя. Это обусловливает важность мер правового регулирования в сфере применения цифровых технологий в области государственного управления. Таким образом, можно заключить, что правовое регулирование использования информационных технологий в деятельности органов исполнительной власти направлено на обеспечение оказания различных государственных услуг, в том числе в электронной форме. Кроме того, правовое регулирование в исследуемой сфере, позволяет модернизировать процесс внутриорганизационного управления, с целью повышения его прозрачности, быстроты и т.д.

По нашему мнению, существует необходимость в постоянном совершенствовании и развитии направлений повышения эффективности системы комплексных административно-правовых средств. Так, важнейшие методы правового регулирования – принуждение, разрешительный и регистрационный, показывают недостаточную эффективность в условиях цифровой реальности.

[29] Чаннов С.Е. Большие данные в государственном управлении: возможности и угрозы // Журнал российского права. №10. 2018. С. 116.

Это во многом связано сложностью урегулирования отношений в информационной сфере и несовершенством законодательных конструкций.

Резюмируя, важно отметить, что применение цифровых технологий при осуществлении государственного управления является неотъемлемым атрибутом современного государства. Это требует развития соответствующих правовых основ. Существующие правовые регуляторы зачастую показывают неспособность регулировать новые отношения в условиях цифровой реальности. Цифровая трансформация меняет сам подход в организации государственного управления, так как происходит качественное его изменение.

Однако цифровые технологии в государственном управлении могут использоваться не только для целей оказания государственных услуг. Их сфера применения является намного более широкой.

Учитывая опыт зарубежных государств, в государственном управлении могут применяться такие технологии, как «большие данные», блокчейн, искусственный интеллект и т.д. Видится, что применение цифровых технологий в государственном управлении позволит не только повысить его эффективность, но и будет способствовать оптимизации расходов государства. Однако процесс их применения должен опираться на действенные правовые основы.

ГЛАВА 2. ЭКСТРЕМИЗМ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

2.1. Новые вызовы и угрозы информационной безопасности в мировом сообществе

Развитие информационных технологий и стремительная модернизация информационной инфраструктуры обеспечили невероятный прорывной потенциал в сфере использования и применения ИКТ на революционно новых принципах, открывая новые сферы их применения. История появления и развития научных технологий показывает, что большинство инновационных изобретений, вне зависимости от их первоначального предназначения, всегда адаптировались для применения в военных целях.

Более того, многие изобретения последней четверти двадцатого века были результатом разработок в военной сфере. Ракета-носитель, посредством которого человечество шагнуло в космос, изначально конструировался как средство доставки ядерных боеголовок; интернет, без которого сложно представить жизнь современного человека, так же первоначально разрабатывался в США специалистами Агентства по перспективным оборонным научно-исследовательским разработкам США (DARPA) как канал коммуникации во время военных действий.

XX век по праву можно считать столетием великих научных открытий и изобретений. Последние три десятилетия наблюдается революционный прорыв в сфере информационно-коммуникационных технологий, которые оказали трансформирующее влияние на все сферы человеческой деятельности, проникая во все социальные процессы, начиная от повседневного быта человека и заканчивая системами управления государственных органов и вооруженными силами государства. Повсеместное использование автоматизации, больших данных (big data), интернета вещей (internet of things) и облачных сервисов приближает наступление пика четвертой индустриальной революции.

Такая корреляция социальных и политических процессов с ИКТ сделала информационную сферу новой платформой для противоборства, которое может проходить по различным направлениям как во время военных действий, так и в мирное время. Это поставило мировое сообщество перед объективной необходимостью по выработке мер обеспечения информационной безопасности.

В настоящий момент данной проблематике уделяется много внимания, тем не менее, до сих пор не существует международной нормативно-правовой базы, регулирующей пределы применения ИКТ в военных целях. Во многом это продиктовано несовпадением взглядов различных государств в определении «информационной безопасности». Также отсутствует согласие исследователей в определении терминов связанных. В публикациях некоторых специалистов данное явление поочередно описывается словом «информационная безопасность» и «кибербезопасность».

При подробном рассмотрении данного вопроса отождествление этих терминов не корректно. Первый термин является более всеобъемлющим, включая в себя как информационно-технологический, так и психологический компонент, в то время как термин «кибер» является частью более пространного понятия «информационный».

Причиной поисков компромиссов и выработки международных правовых норм, регулирующих деятельность в информационном пространстве, стала возможность применения ИКТ в целях не совместимых с международной безопасностью. Применение информационных технологий (далее – ИТ) в военных целях в первую очередь подразумевает оснащенность высокоточного оружия (далее – ВТО) информационными электронными компонентами. Информационные параметры обеспечивают ВТО значительным преимуществом над конвенциональным оружием. Наличие такого «умного оружия» де юре не выходит за правовые рамки, регулирующие применение обычных вооружений, но де факто обладает значительными преимуществами над конвенциональными вооружениями.

Впервые практическое использование ВТО было наглядно продемонстрировано ВВС США во время операции «Буря в пу-

стыне» в Ираке в 1991 г. Наряду с использованием ВТО совершалось применение средств радиоэлектронной борьбы (далее – РЭБ), посредством которого осуществлялось нарушение работы систем Противовоздушной обороны (далее – ПВО) Ирака. Кроме операции Буря в пустыне массированное применение ВТО демонстрировалось во время Югославского конфликта (1999 г.), в Афганистане (2001 г.), в Иракской кампании (2003 г.), в Сирии (2012 г. – наст. время).

Помимо применения в военных целях информационное противоборство (далее – ИП) может вестись в мирное время. Слово «мирное» следует понимать с некоторой степенью условности, так как любая информационная атака подразумевает нанесение деструктивного эффекта на объект информационной атаки.

Данное направление ИП может использоваться для вмешательства в дела суверенного государства, целью которого является нарушение общественного порядка, провокации общественных волнений, подрыв доверия общества к правящей элите, разжигание межнациональной, межрелигиозной неприязни и других ксенофобских настроений.

Одним из основных способов такого вида ИП является информационно-психологическое воздействие (далее – ИПВ) на общественное сознание граждан, для создания иллюзорных представлений, не соответствующих действительности. Ярким примером применения ИПВ являются события Арабской весны, начавшиеся в Тунисе в 2011 г. и спровоцировавшие целый ряд революций в арабском мире, которые привели к дестабилизации Ближневосточного региона.

Участие в Арабской весне третьих стран и ИПВ на массовое сознание граждан не оставляет сомнений. По мнению Чрезвычайного и полномочного посла Российской Федерации в Тунисе А.Б. Подцероб, информационная пропаганда на фоне комплекса накопившихся экономических и социально-политических проблем явилась детонатором протестных выступлений Арабской весны.

Современное международное право, сохраняя свое значение важнейшего нормативного регулятора межгосударственных отношений, призванного обеспечить стабильность международного порядка и прежде всего поддержание международного мира

и безопасности, сталкивается с необходимостью включения в орбиту своего воздействия новых сфер отношений, формирующихся, в том числе, под воздействием научно-технологического прогресса.

Одним из технологических феноменов современности, оказывающих глубокое влияние на жизнедеятельность человека и облик мира в целом, является Интернет, представляющий собой сложную единую информационно-техническую систему, включающую наряду с техническим и социальный компонент.

Развитие интернет-технологий, расширяя социальные сферы его применения, по признанию специалистов, диверсифицирует правовое регулирование значительного числа общественных отношений как на национальном, так и на международном уровне, а также вызывает необходимость правового регулирования новых общественных отношений.

Разумеется, становление международно-правового регулирования новых сфер международных отношений – процесс не одномоментный, занимающий продолжительное время, требующий внимательного изучения государствами всех сторон и аспектов новых явлений. Такое отношение характерно и для реакции международного права на Интернет.

До настоящего времени Интернет так и не стал предметом международно-правового регулирования или хотя бы международно-правового управления. Конвенция Совета Европы о преступности в сфере компьютерной информации 2001 г. затрагивает лишь один, пусть и важный, вопрос, связанный со стремлением наладить международное сотрудничество в борьбе с использованием Интернета в преступных целях.[30]

Между тем сегодня ни у кого не вызывает сомнений, что Интернет имеет международное значение как в связи с его трансграничным функционированием и использованием, так и в связи с тем, что международное сообщество признает важную роль Интернета, открывающего широкие возможности для развития цивилизации и построения глобального информационного об-

[30] Конвенция о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.) / [Электронный ресурс] // Режим доступа: https://base.garant.ru/4089723/

щества. В связи с этим для разработки концепции международно-правового регулирования Интернета необходим анализ его использования государствами в сфере межгосударственных отношений.

Среди этих вопросов на первый план выступают проблемы обеспечения международного мира и безопасности в контексте использования информационно-коммуникационных технологий (ИКТ). Государства еще в 1990-х гг. осознали негативный аспект неконтролируемого использования ИКТ в международных отношениях. Однако продвижение вперед в деле создания международно-правового механизма противодействия угрозам международной информационной безопасности особо не ощущается, он так и не сформирован до настоящего времени.

К основным угрозам в области международной информационной безопасности (далее – МИБ) следует отнести использование ИКТ в преступных целях, в том числе и террористических актах. Опасения применения ИКТ во враждебных целях подтвердились в 2010 г., когда произошла атака на ядерную программу Ирана. Вирус Stuxnet (Стакснет) поразил 1368 из 5000 центрифуг по обогащению урана, что привело к повреждению системы охлаждения АЭС. Мировое сообщество заговорило о войнах шестого поколения.

Сложившаяся на международной арене ситуация вызвала объективную необходимость выработки комплекса мер по обеспечению МИБ. Первым инициатором сотрудничества в обеспечение МИБ выступила Россия в 1998 г. Это положило начало двухстороннего сотрудничества России и США.

В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы также отмечено, что «международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети "Интернет", не установлены».[31]

[31] Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы / [Электронный ресурс] // Режим доступа: https://sudact.ru/law/ukaz-prezidenta-rf-ot-09052017-n-203/strategiia-razvitiia-informatsionnogo-obshchestva-v/

Новизна правовых проблем, с которыми сталкивается человечество в сфере использования ИКТ, обусловливает теоретическую и практическую значимость систематизации фактического материала для формирования категориального аппарата. Одной из таких ключевых задач видится разработка международно-правовых вопросов определения угроз международной информационной безопасности, или киберугроз.

В стратегических документах и законодательных актах России используется различная терминология для обозначения сети Интернет или информационного пространства. Так, в Федеральном законе от 27 июня 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» употребляются термины «информация», «информационная система», «информационно-телекоммуникационные сети» и др.

В Концепции внешней политики Российской Федерации 2016 года встречаются термины «информационное пространство», «информационно-телекоммуникационная сеть «Интернет». В Стратегию развития информационного общества в Российской Федерации на 2017-2030 годы введены понятия «информационное пространство», «объекты критической информационной инфраструктуры».

В то же время в официальных документах наряду с понятием «Интернет» или «информационное пространство» используются выражения с приставкой «кибер», подчеркивающие связь объектов или действий с Интернетом. Например, в Концепции внешней политики Российской Федерации 2016 г. при характеристике вызовов и угроз, имеющих трансграничную природу, упоминается «киберпреступность».

В свою очередь, гл. 28 УК РФ называется «Преступления в сфере компьютерной информации», в ней, например, дается определение составу преступления «неправомерный доступ к охраняемой законом компьютерной информации» (ст. 272) или «создание, использование и распространение вредоносных компьютерных программ» (ст. 273).

В зарубежной и отечественной литературе для обозначения Интернета и производных от него выражений все шире прибегают к термину «киберпространство» и иным словам, содержащим

приставку «кибер». Понятия «угрозы государственной, экономической и общественной безопасности, исходящие из информационного пространства» (см. Концепцию внешней политики Российской Федерации 2016 г.) и «киберугрозы», близки, но не тождественны, тем не менее, в дальнейшем для определения предмета исследования будет использоваться термин «киберугроза».

В Доктрине информационной безопасности Российской Федерации 2016 г. для характеристики применения информационных технологий в неблагоприятных для национальных интересов страны целях используются весьма нейтральные выражения «информационное воздействие» или «информационно-техническое воздействие». Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» содержит два понятия: «компьютерная атака» и «компьютерный инцидент».

В Докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее – Доклад) встречаются более определенные понятия, например, «злонамеренное использование ИКТ», «пагубные нападения», «вредоносные нападения». В этом Докладе отмечаются тревожные тенденции в глобальной ИКТ-среде, создающие угрозу для всех государств, а злонамеренное использование ИКТ может нанести ущерб международному миру и безопасности.

Ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей, опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной.

Существует все более реальная опасность использования ИКТ для террористических целей. Многообразие злонамеренных негосударственных субъектов, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу. Если понятие «использование ИКТ» без эпитета «злонамеренное» еще может свидетельствовать о правомерном поведении субъектов в киберпространстве, то термин «нападение» без каких-либо дополнительных характеристик, указыва-

ющих на его противоправность, непроизвольно ассоциируется с недружелюбным действием, способным причинить ущерб.

Для объективной оценки международно-правового регулирования противодействия киберугрозам необходимо иметь в виду, что оно находится еще на начальном этапе развития. Первые международные договоры о сотрудничестве государств в борьбе с киберугрозами разрабатываются и принимаются на региональном уровне. Так, Совет Европы принял ряд международно-правовых актов по сотрудничеству в сфере информации (Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 г. и др.), в их числе упомянутая выше Конвенция о преступности в сфере компьютерной информации.

Данный документ обязывает участников криминализировать преступные виды использования компьютерных сетей и электронной информации, которые создают угрозу законным интересам государств и частных лиц в сфере использования и развития информационных технологий.

Конвенция о преступности в сфере компьютерной информации не единственный документ такого рода. В 2014 г. была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных. В других регионах также приняты международно-правовые акты или еще идет обсуждение возможности заключения подобных документов.

Такого рода киберугрозы можно нейтрализовать с помощью мер, предусмотренных национальным уголовным правом, при необходимости путем международного сотрудничества в уголовно-правовой сфере. Субъектами, создающими такого рода угрозы, являются частные лица (физические или юридические), соответственно, хотя они регулируются международными договорами, они не затрагивают сферу международной безопасности.

Повышению уязвимости в условиях взаимозависимого мира может послужить разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами. Г. Кершишниг, посвятивший свое исследование проблеме киберугроз, использует ряд терминов, которые должны обозначить различную степень опасности для международной информационной

безопасности случаев недружественного проникновения в киберпространство.

В качестве наиболее общего понятия он использует выражение «кибервмешательство» (cyberintrusion), определяя в качестве «киберинцидентов» неприятные происшествия в киберпространстве, виновники которых так и не были обнаружены и преданы огласке. Наконец, следующей по степени опасности разновидностью кибервмешательства он называет кибернападение или кибер-атаку (cyberattack), а самой опасной – кибервойну (cyberwar). Встречается также выражение «кибероперации».

Проблема квалификации кибератаки или атаки на компьютерные сети как действия, подлежащего оценке в соответствии с международным правом, на сегодняшний день является особенно актуальной. События последнего времени, особенно пропагандистские кампании, развернувшиеся в результате гибридной войны западных государств против России, в том числе недоказанные, ничем не подтвержденные голословные обвинения нашей страны во вмешательстве во внутренние дела, в частности в выборы в США, ФРГ и других стран, наглядно свидетельствуют об острой необходимости анализа категорий кибероперации, кибератак и кибервмешательства с точки зрения международного права.

Рассматривая понятие кибератаки как способ применения имеющихся технологических возможностей государством или даже негосударственными субъектами против других государств или негосударственных образований, необходимо исходить из устоявшихся правовых или технических понятий и категорий. Не останавливаясь подробно на анализе понятий «кибервмешательства» и его возможных форм, а также дефиниций «кибероперации» и «кибернападения» («кибератаки») с точки зрения международного права, что бесспорно заслуживает отдельного и подробного рассмотрения с учетом как действующих норм международного права, так и особенностей киберпространства, в качестве иллюстративного примера рассмотрим возможность допущения юридического определения кибератак как разновидности применения силы государством в нарушение действующего международного права.

Следует признать, что на сегодняшний день подобное допущение является не столь очевидным, как это может показаться на первый взгляд, хотя нельзя исключать возможности его использования при достижении достаточного уровня согласия государств.

На сегодняшний день уже были зафиксированы единичные случаи кибератак, оказавших влияние на жизнь и здоровье человека, а также вызвавших риски экологических катастроф. Вместе с тем, деструктивный потенциал кибератак становится все более очевиден, особенно в области геополитических угроз.

Например, кибератака в Турции в декабре 2015 года повлияла на работу сетей, используемых банками, средствами массовой информации и правительственными учреждениями страны. Позднее в том же месяце впервые в результате кибератаки на электроэнергетическую систему были выведены из строя энергораспределительные системы на Украине, оставив без электричества 230 000 жителей. Эта атака также была нацелена на телефонную систему страны, что помешало потребителям сообщать о перебоях с электричеством и в результате затруднило усилия по восстановлению энергоснабжения.

Весной и летом 2017 года компьютеры многих компаний по всему миру поразила серия вирусов-шифровальщиков под названием WannaCry и Petya, которые вызвали операционные сбои и простои как в цифровой, так и в операционной деятельности крупных международных и российских компаний. В дополнение к этому риски, связанные с массовой утечкой данных, усиливают озабоченность потенциалом влияния кибератак на глобальную экономику.

Широкий спектр комментариев о киберугрозах, от откровенного преувеличения и создания мифа о кибермагеддоне до прямо противоположной позиции о будничном характере большинства кибератак, лишь создают информационный беспорядок и вводят руководство компаний в заблуждение. Гораздо более продуктивной стала бы рациональная международная дискуссия, в результате которой руководители компаний получили бы практические рекомендации по повышению устойчивости своих организаций к кибератакам.

Как показали ситуационные исследования катастроф некибернетического характера, события, которые развиваются по каскадному принципу, обычно начинаются с нарушения энергоснабжения, что приводит к поражению ряда систем мгновенно или в течение суток. Таким образом, чаще всего на устранение исходной проблемы, прежде чем она распространится по каскадному принципу, имеется ничтожно малое количество времени.

Взаимозависимость между критическими или некритическими ИТ-инфраструктурами обычно остается незамеченной до возникновения аварийной ситуации. Множество людей – особенно в Японии, США, Германии, Великобритании и Южной Корее – обеспокоены возможностью совершения кибератак с территории других стран.

Инструменты для совершения кибератак стремительно развиваются по всему миру. Менее крупные страны нацелены на развитие возможностей, подобных тем, которыми обладают более крупные державы. Утечка хакерских инструментов Агентства национальной безопасности США открыла этот сложнейший инструментарий для хакеров. Говоря о последствиях кибератак, большинство компаний, ставших их жертвами, утверждает, что не в состоянии точно установить лиц, совершивших преступление.

В мае 2017 года лидеры стран «Большой семерки» взяли на себя обязательство сообща и вместе с другими партнерами работать над противодействием кибератакам и снижением их воздействия на критически важную инфраструктуру и общество. Спустя два месяца лидеры стран «Большой двадцатки» вновь признали необходимость обеспечения кибербезопасности и повышения доверия к цифровым технологиям. Задача, стоящая перед нами, масштабна.

Как отметили в Международном союзе электросвязи ООН, индекс за 2020 год «подтверждает, что страны работают над повышением уровня своей кибербезопасности, несмотря на связанные с COVID-19 проблемы и стремительный переход повседневной деятельности и социально-экономических услуг в цифровую сферу».[32]

[32] Глобальный индекс кибербезопасности Global Cybersecurity Index (GCI). / [Электронный ресурс] // Режим доступа: https://www.tadviser.ru/index.php/

Для многих людей такие риски являются реальными. Исследование, проведенное Pew Research Center, выявило, что абсолютное большинство американских граждан в ближайшие пять лет прогнозируют крупномасштабные кибератаки на общественную инфраструктуру США или на банковскую и финансовую системы. Большинство специалистов в области информационной безопасности полагают, что критически важная инфраструктура США подвергнется кибератаке в ближайшие два года.

Отсюда возникает необходимость для всех организаций – независимо от того, в какой степени готовности они, по их собственному мнению, находятся, – определять и проверять успешность достижения своих стратегических целей в сфере кибербезопасности. Как сказано в отчете Национального консультативного совета Белого дома по инфраструктуре за август 2017 года, многие системообразующие компании в США не практикуют базовую кибергигиену, несмотря на наличие и доступность соответствующих эффективных инструментов и практики.

Представляется, что по мере достижения прогресса в разработке международно-правового понимания использования ИКТ в контексте поддержания международной безопасности он вполне может выступить в качестве ключевой категории в решении задачи международно-правовой квалификации кибератаки.

Однако нельзя забывать прошлый опыт, когда делались попытки расширительного толкования понятия силы, включавшего не только вооруженную силу государства, но и экономическую, информационную и другие составляющие внешнеполитического потенциала государства. Они были подвергнуты критике на том основании, что п. 4 ст. 2 Устава ООН запрещает применение исключительно вооруженной силы в международных отношениях, а все иные составляющие внешнеполитического потенциала не входят в сферу действия этой нормы.

Кибератаки по определению нацелены на информацию и информационные системы. Однако они могут быть разделены на те, которые нацелены на информационные системы для того, чтобы повлиять на аппаратные средства и другие физические аспекты сети, и те, которые нацелены на информацию как таковую. Когда объектом нападения в конечном счете является физический

объект, как это происходит, например, с манипулированием программным обеспечением управления скоростью вращения ядерных центрифуг или иных объектов критических информационных систем, эффекты кибератаки легче вписываются в привычные представления о применении силы. Более сложная проблема возникает тогда, когда целью кибератаки является сама информация.

В частности, когда последствием кибератаки не является разрушение собственно информации, а скорее причинение ущерба функционированию информационного объекта в такой степени, что теряется возможность пользоваться информацией, содержащейся в данном объекте. Оценка последствий такого нападения, очевидно, будет зависеть от характера системы, которая подверглась кибератаке.

Так, последствия порчи информации в системе управления воздушным движением, очевидно, будут более катастрофичны, чем те, которые могут произойти в каких-либо других информационных объектах, например, в банках или небольших промышленных предприятиях.

По мнению некоторых специалистов, первый пример будет совершенно точно рассматриваться как применение силы в общепринятом в международном праве смысле, а последний скорее всего будет восприниматься как причинение экономического ущерба. Отсюда делается вывод: принимая во внимание возможные негативные последствия, тот факт, что нападение на системы управления воздушным движением выльется в серьезный урон и возможные человеческие потери, явно позволяет отнести его к разновидности применения силы в нарушение п. 4 ст. 2 Устава ООН.

Таким образом, угроза защиты информации обусловила существование различных средств обеспечения информационной безопасности. Одна из главных характеристик информационной системы России непосредственно связана с уровнем обеспечения информационной безопасности.

Информационная безопасность является важнейшей частью государственной системы безопасности и России. «Основы государственной политики Российской Федерации в области меж-

дународной информационной безопасности на период до 2020 года» указывают на то, что главной угрозой в сфере международной информационной безопасности является использование информационных и коммуникационных технологий:

- в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

- в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

- для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

- для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ. [33]

Проблема информационной безопасности в последние годы начала активно решаться и на уровне национального российского законодательства. Была переработана и изменена гл. 28 УК РФ «Преступления в сфере компьютерной информации». В настоящее время внесены поправки в законы «О персональных данных» и «Об информации, информационных технологиях и о защите информации».

Особого внимания заслуживает Конвенция о международной информационной безопасности, которая определяет термин «информационная война» как «противоборство между двумя или

[33] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года / [Электронный ресурс] // Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70541072/

более государствами в информационном пространстве с целью нанесения ущерба информационным системам», «подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны».

В новой Доктрине определена защита интересов личности, общества и государства от осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств.

В Доктрине особое внимание уделяется угрозам, связанным с использованием механизмов информационного воздействия на индивидуальное, групповое 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. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

На сегодняшний день важным представляется проект Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, где под информационной безопасностью понимается «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Для решения вопросов международно-правового сотрудничества в информационной сфере представляется результативной работа в следующих направлениях:

- запрещение разработки, распространения и применения «информационного оружия»;

- обеспечение безопасности международного информационного обмена, в условиях сохранности информации при ее переда-

че по национальным телекоммуникационным каналам и каналам связи;

- координация деятельности правоохранительных органов стран по предотвращению компьютерных преступлений;

- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли.

Касаясь деятельности Российской Федерации на платформе ООН в рамках создания международной правовой базы информационной безопасности, следует подчеркнуть, что Россия еще осенью 1998 года на сессии Генеральной Ассамблеи ООН призывала к объединению усилий для противодействия использованию информационно-коммуникационных технологий в противоправных военно-политических, террористических и иных преступных целях (так называемая «триада» угроз).

Однако эксперты и политики «утонули» в многолетних бесплодных дискуссиях, в которых объективность оценки ситуации подменялась идеологическими установками. Только спустя 12 лет, в 2010 году в докладе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности была зафиксирована упомянутая «триада» угроз.

Была принята резолюция «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности», где вопросы распространения и использования информационных технологий и средств затрагивали интересы всего международного сообщества.[34]

Генеральная Ассамблея призвала государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных угроз, возникающих в этой сфере, исходя из необходимости, сохранить свободный поток информации.

[34] Резолюция Генеральной Ассамблеи Организации Объединенных Наций от 8 декабря 2010 года №A/RES/65/41 «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» / [Электронный ресурс] // Режим доступа: https://online.zakon.kz/Document/?doc_id=31094419

В январе 2015 года государствами-членами ШОС были внесены в качестве официального документа в ООН «Правила поведения в области обеспечения международной информационной безопасности».

В рамках данных инициатив в Российской Федерации приняты «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утвержденные Указом Президента Российской Федерации от 24 июля 2013 года. Здесь определены основные угрозы в области международной информационной безопасности, цели, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности, а также механизмы их реализации.

Положения Указа Президента Российской Федерации №Пр-1753 детализируют отдельные положения Стратегии национальной безопасности Российской Федерации, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов.

Подписаны Соглашение между Правительством Российской Федерации и Правительством Кубы о сотрудничестве в области обеспечения международной информационной безопасности, а также Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности.

Участники данных Соглашений осуществляют сотрудничество и свою деятельность в международном информационном пространстве в рамках заключенных ими Соглашений так, чтобы эта деятельность способствовала социальному и экономическому развитию государств, была совместима с задачами поддержания международной безопасности и стабильности, а также соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека.

В основах государственной политики Российской Федерации в области международной информационной безопасности на пе-

риод до 2020 года, утвержденных Указом Президента Российской Федерации от 24.07.2013 года, международная информационная безопасность понимается как состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. И государства должны бороться с использованием скрытых вредоносных функций.

Для России, как и для большинства государств-членов ООН, важно закрепить в цифровой сфере принципы неприменения силы, уважения государственного суверенитета, невмешательства во внутренние дела других государств, соблюдения основных прав и свобод человека.

Ощущая все более настойчивый запрос со стороны международного сообщества, Россия с широким кругом единомышленников из всех регионов мира неоднократно предлагала разработать и рекомендовать к принятию Генассамблеей ООН универсальные правила ответственного поведения государств в информационном пространстве, отражающие данные принципы. Именно эту идею Россия продвигала в последней ГПЭ.

Россия намерена заключить двусторонние межправительственные соглашения о предотвращении эскалации компьютерных инцидентов с рядом государств.

В перспективе Москва рассматривает возможность внесения на рассмотрение Генассамблеи ООН новой коллективной резолюции по информационной безопасности. В этой резолюции будут учтены конкретные положения по механизмам дальнейших переговоров в рамках ООН по вопросам международной информационной безопасности. Основу документа могут составить уже согласованные международным сообществом в рамках ООН и ОБСЕ полезные нормы ответственного поведения государств, а также меры доверия, полагает эксперт.

Внесение этого документа на обсуждение Генеральной Ассамблеи ООН позволило бы заложить прочную основу для формирования глобальной и поистине универсальной системы МИБ и подключить к выработке этих жизненно важных международных договоренностей практически все страны – члены ООН.

2.2. Информационный аспект экстремизма и деструктивные тенденции в СМИ

В современных условиях международная информационно-телекоммуникационная сеть Интернет все чаще используется экстремистскими организациями в целях размещения запрещенных материалов. При помощи глобальной сети Интернет и возможностей компьютерных технологий идеологи экстремистских и террористических формирований приобрели возможность воздействия на сознание людей, и прежде всего молодежи.[35]

Данная проблема имеет планетарный масштаб и представляет особую актуальность для России, выступающей одним из основных акторов мирового политического процесса. Таким образом, в последнее время происходит обострение проблематики противодействия экстремизму, который в настоящее время рассматривается не только как проблема государственного значения, но и в качестве угрозы национальной безопасности Российской Федерации.

По мнению авторов, решить проблему противодействия террористическим и экстремистским организациям довольно сложно. Однако эффективность работы в данном направлении во многом зависит от действенной и современной правовой базы. Особая роль в блоке нормативно-правовых актов в сфере противодействия экстремизму принадлежит нормам уголовного права, которое, в свою очередь, обладает рядом недостатков. Авторы отмечают необходимость разработки общегосударственной комплексной программы, охватывающей не только правоохранительный, но и политический, социальный, экономический, правовой, идеологический, пропагандистский, информационный, оперативно-розыскной и другие аспекты.[36]

[35] Золоев С.Т., Багаева А.А. Основы реализации государственной политики по противодействию экстремизму и терроризму в современных СМИ и интернет-пространстве // Развитие интеллектуально-творческого потенциала молодежи: из прошлого в современность. Материалы I Международной научно-практической конференции / Под общ. ред. проф. С.В. Беспаловой. 2018. С. 276.

[36] Золоева З.Т., Койбаев Б.Г. Некоторые проблемы правового противодействия экстремистским проявлениям в информационно-телекоммуникационной сети Интернет // Гуманитарные и юридические исследования. 2018. №4. С. 170-175.

Наращиванию агрессивных, экстремистских, преступных тенденций в российском обществе зачастую способствуют российские средства массовой информации (коммуникации). Особенно сильно данное влияние на сознание и поведение молодежи, так как посредством СМИ (главным образом сети Интернет) экстремистские и террористические организации осуществляют рекрутинг неофитов, в основном из молодежной среды, пропагандируя свои разрушительные идеи. Поэтому актуальна проблема поиска возможностей использования профилактического потенциала СМИ для противостояния экстремистским и террористическим организациям и группам.

Сущностью массовой коммуникации как деятельности (массово-коммуникативной деятельности) является воздействие на общество путем внедрения в массовое сознание определенной системы ценностей.[37] Основные компоненты массовой коммуникации были представлены в модели Г. Лассуэлла: кто сообщает – что – по какому каналу – кому – с каким эффектом.[38] При этом эффект от полученной информации как результат деятельности средств массовой коммуникации (СМК) является основополагающим звеном в данной схеме.

При этом данный эффект зачастую бывает негативным и даже экстремистским. Созданный на наших глазах благодаря Интернету симулятор реального мира несет в себе все пороки и противоречия, характерные для своей матрицы – физического социума, причем работает как их усилитель. Негативный фактор, попав из социума в кибернетическое пространство, не просто проецируется там, но, модифицируясь и усиливаясь, возвращается к своему прототипу по принципу эха, оказывая на него деструктивное воздействие. В полной мере это относится к природе политического экстремизма.[39]

---

[37] Науменко Т.В. Социология массовой коммуникации. СПб., 2005. С. 56.

[38] Основы теории коммуникации / Под ред. М.А. Василика. М., 2003. С. 443.

[39] Морозов И.Л. Политический экстремизм: особенности эволюции при переходе от индустриального общества к информационному: Монография. Волгоград, 2007. С. 36.

Экстремизм, традиционно достигавший своих целей путем примитивного силового давления, сегодня все чаще прибегает к новейшим интеллектуальным достижениям. От обычных насильственных мер он перешел к информационной манипуляции сознанием.[40]

Тотальная информатизация всех сторон жизни и деятельности человека не только ускоряет производственные процессы, открывает принципиально новые горизонты личностного развития, но и порождает новые опасности и негативные факторы. К последним относится принципиальная уязвимость постиндустриального общества с точки зрения информационного противодействия, которое может принять характер как межгосударственных войн, так и «выяснения отношений» внутриэлитных группировок. От этой тотальной информатизации новые рычаги воздействия получает в том числе и организованная преступность.

Информационное пространство понимается как сфера человеческой деятельности, связанная с созданием, преобразованием и потреблением информации, включает в себя индивидуальное и общественное сознание, а также всю совокупность информационных ресурсов данного общества. Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

И в мире в таких условиях привычно «мирные» институты (средства массовой коммуникации) являются проводниками различных идеологий и оружием в войнах нового поколения – «информационных», которые, в свою очередь, могут рассматриваться как реализация конфликтов идеологий.[41]

В России одной из первых фундаментальных попыток определить суть понятия информационной войны и способы сохранения государственного суверенитета в области культуры и информации стал доклад, подготовленный в 1996 г. аналитической группой Федеральной службы безопасности РФ для Президента России.

[40] Экстремизм в среде петербургской молодежи: анализ и проблемы профилактики / Под ред. А.А. Козлова. СПб., 2003. С. 169.

[41] Кирюшин А.Н., Асташова А.Н. Информационная война: сущность и содержание // Экстремизм, конфликты и войны: история и современность: Труды Междунар. конф. Воронеж, 2010. С. 196.

Доклад имел название «Основные угрозы в сфере информационной безопасности Российской Федерации». В этом докладе отмечается, что информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов Российской Федерации, чем диктуется необходимость создания развитой и защищенной информационной среды общества.

В традиционном противостоянии политических оппонентов растет значимость информационно-психологического воздействия, а в экономике растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации.

В сфере духовной жизни возникает опасность развития потребительской идеологии, тотальной коммерциализации культуры, распространения идей насилия и нетерпимости, воздействия на психику разрушительных форм мифологизированного сознания.

По мнению А.Н. Кирюшина и А.Н. Асташовой, информационная война – это целостная стратегия (спланированная система действий), направленная на достижение гуманитарного порабощения одних групп людей другими, основанная на манипулировании сознанием, включающая определенные методы психологического воздействия с целью изменения взглядов, мнений, ценностных ориентаций, настроений, мотивов, установок, стереотипов поведения, а также групповых норм, массовых настроений, общественного сознания в целом.[42] Для этого используются электронные СМИ, функционирующие в глобальном безграничном пространстве.

О.О. Антименко выделяет несколько аспектов, которые все сильнее вовлекают СМИ в процесс информационной борьбы.

Во-первых, любое сообщение СМИ для того, чтобы привлечь к себе внимание, должно носить яркий эмоциональный след, быть реальной или вымышленной сенсацией. В погоне за рейтингами большое внимание уделяется масс-медиа различным происшествиям и катастрофам, что становится ключевым алгоритмом интерпретации действительности. И здесь, как это ни печально,

[42] Асташова А.Н., Кирюшин А.Н. Психологическая война как война будущего // Экстремизм, конфликты и войны: история и современность: Труды Междунар. конф. Воронеж, 2010. С. 188.

стремления СМИ совпадают с интересами экстремистских и террористических организаций, основная задача которых не просто совершить теракт, а придать этому событию возможно более широкий резонанс, произведя, таким образом и в первую очередь, акт психического устрашения и дезорганизации.

Во-вторых, организационная структура масс-медиа открывает широкий простор для использования их со стороны различного рода, в том числе и экстремистских, организаций, и объясняет ту легкость, с которой сообщество профессионалов в сфере изготовления и передачи массовой информации принимает навязанные им теми или иными силами («заказчиками») правила игры.[43]

В настоящее время информационно-психологическую войну ведут различные экстремистские и террористические организации, имеющие целью воздействие своих идей на как можно большее число людей (особенно в молодежной среде) и укрепление своего влияния. Как следствие – то, что в последние годы происходит дальнейшее развитие неофашизма, неонацизма, агрессивного национализма, ксенофобии, антисемитизма в молодежной среде России, стран СНГ, Балтии, Запада и Востока.

Развитие глобальных информационных компьютерных сетей и кибернетических систем, неподконтрольных государству (точнее – слабо контролируемых ввиду колоссального объема данных, развития средств криптографии и маскировки значимой информации в потоке обыденных сообщений), позволило экстремистским и террористическим организациям эффективно решить сразу два блока задач.

Прежде всего значительно упростилась система управления боевыми отрядами, процедура адресного рекрутинга боевиков и поиска адептов. По спутниковой беспроводной интернет-связи стало возможно разместить объявления о потребности в боевиках для проведения той или иной акции, провести переговоры со всеми желающими, «отфильтровать» провокации со стороны спецслужб, произвести закупки оружия, денежные переводы на оплату услуг боевиков и проконтролировать результаты проведения

[43] Антименко О.О. Экстремизм и СМИ: спасет ли нас общественный контроль? // Экстремизм и средства массовой информации: Мат-лы Всерос. науч.-практ. конф. / Под ред. В.Е. Семенова. - СПб., 2006. С. 151.

заказанной операции. При этом руководящий штаб террористов находится в состоянии неуязвимости для служб безопасности той страны, против которой готовится диверсия.[44]

С развитием электронных сетей террористы получают качественно новую возможность для пропаганды своих идей, для показательной полемики с официальными государственными структурами, для дискредитации и дезавуирования заявлений официальных властей. Информация, размещаемая в Интернете, отличается адресностью, неподцензурностью и высокой устойчивостью в качестве пропагандистской единицы. Компьютеризация (автоматизация) административно-управленческих процессов существенно повышает уязвимость системы путем использования чрезвычайно дешевых и доступных методов информационно-компьютерных диверсий. Под потенциальный удар в первую очередь попадают наиболее развитые страны, с высокой степенью разработанности открытых информационных систем – более 50% пользователей Интернета проживают в США и Канаде.[45]

Сущность информационно-психологического терроризма заключается в следующем: дезинформация; внушение через СМИ нравственно-этических и поведенческих стереотипов, противоречащих традиционным для данного народа нравственным ценностям, социально-бытовым традициям и нормам; целенаправленные публикации, радио- и телепрограммы, извращающие исторические факты, нравственные ценности и культурные традиции народа; внушение через СМИ катастрофизма, неуверенности, страха; методическая дискредитация государственных и социальных институтов; внушение комплекса вины представителям другого социального слоя, другой религии, другой этнической группы, гражданам другого государства; внушение комплекса неполноценности этнической группе, гражданам какого-либо государства, представителям какой-либо культуры или конфессии.[46]

При этом опасение, по мнению О.В. Туманян, вызывает не

[44] Морозов И.Л. Политический экстремизм: Учеб. пособие. Волжский, 2008. С. 39.

[45] Морозов И.Л. Политический экстремизм: Учеб. пособие. Волжский, 2008. С. 39.

[46] Терроризм: история и современность / Кофман Б.И., Миронов С.Н., Сафаров А.А., Сафиуллин Н.Х. - Казань, 2002. С. 92.

только количество информации о насилии, но и способ подачи материала: акцентирование внимания на самом акте насилия как процессе, его смакование без нравственного осуждения агрессора и т.п. Эпатаж и культурный шок – обыденные реалии функционирования СМИ, основанные на коммерции и рынке.

Обилие и популярность видеопродукции, которая эксплуатирует темы насилия, жесткой эротики, ведут к усилению агрессивности всех слоев общества, но в особенности молодежи, т.к. именно она составляет основную аудиторию кинотеатров и видеосалонов. Это приводит к росту девиантного поведения, молодежного экстремизма, выражающегося в пренебрежении к действующим в обществе правилам и нормам поведения, волюнтаризме, культе силы и насилия и др. Учащаются случаи молодежного терроризма, вступления молодежи в различные террористические организации. СМИ оказывают воздействие на образ мышления, на нормы и стандарты поведения людей. Постоянная демонстрация на экране сцен насилия, убийств и т.п. формирует у молодого человека неверные представления об окружающем мире, ощущение неуверенности и страха, создает неверное представление о том, что наиболее эффективный способ решения конфликта – насильственный.

«Виртуальная реальность» в компьютерных играх формирует особый тип сознания и снижает порог дозволенности/недозволенности. Отсутствие стратегического мышления у российский властных структур и эгоистичные интересы СМИ обрекают современное российское общество на рост девиантности (и молодежного экстремизма-терроризма) в стране. [47]

Результаты проведенных исследований (А. Бандура, Э. Донерстайн, Л. Берковиц, А.Ю. Дроздов) позволяют говорить о наличии взаимосвязи между склонностью к просмотру телевизионных сцен насилия и дальнейшим агрессивным поведением по отношению к сверстникам. Дети более подвержены негативному воздействию средств массовой информации, поскольку они, в

[47] Туманян О.В. Современные СМИ как фактор влияния на агрессивное и экстремистское поведение молодых // Актуальные вопросы исследования и профилактики экстремизма. Материалы межд. науч.-практ. конф. / Под ред. А.А. Козлова. СПб., 2004. С. 107.

отличие от взрослых, принимают негативное поведение за образец.[48]

В свою очередь, О.Л. Гнатюк отмечает, что резкая коммуникативная асимметрия (именно в сторону негативной информации) создает огромные возможности для манипуляции массовым сознанием. Девиация становится нормой, а «диффузная» тревожность – устойчивым свойством личности, готовой к поиску образов «новых врагов» как источнику возможной опасности. Одна из основных существующих дисфункций российских СМИ проявляется сегодня как воспроизводство негативной информационной асимметрии. [49]

Социологи констатируют сформированность таких черт массового кризисного сознания, как потеря индивидуальной и групповой идентичности, упаднические настроения, утрата ориентиров и уверенности в себе и в ближайшем будущем, появление социальной апатии, замена ценностной ориентации на целерациональную, снижение доли общекультурных и общечеловеческих ценностей в системе значимостей и смыслов, замена демократических и правовых ценностей на криминальные, замещение принципа социальной справедливости для определенных групп и слоев, усиление социального расслоения.

Алармизм, фрустрационность современных российских СМИ, управляя сознанием и поведением массовой аудитории, снижают ценность человеческой жизни, порог чувствительности к страданиям и смерти, и формируют тип личности – тревожного, но потенциально агрессивного конформиста, нацеливая его на поиски образа «новых врагов», внушая ему фобии и упаднические настроения. С другой стороны, это снижает уровень доверия к самим СМИ.[50]

Американский экономист и политолог Лестер Туроу пишет о том, что средства массовой информации наживают деньги, продавая возбуждение. Нарушение существующих общественных

[48] Татарова С.П. Возможности средств массовой информации в профилактике экстремизма // Экстремизм и СМИ... СПб., 2006. С. 182.

[49] Гнатюк О.Л. Алармизм как негативная асимметрия, или Новая функция российских СМИ? // Экстремизм и СМИ... СПб., 2006. С. 17.

[50] Козлов А.А., Козлов Н.А. СМИ, экстремизм, молодежь // Экстремизм и СМИ... СПб., 2006. С. 17-18.

норм вызывает возбуждение, один из вариантов которого – это громкие террористические акты.

Последствия деструктивного влияния многих СМИ находят свое выражение в снижении чувствительности человеческого сознания к агрессии (феномен равнодушного отношения к жертвам насилия), ослаблении сдерживающих агрессию сил (синдром растормаживания), деформировании восприятия действительности (эффект враждебности). В результате генерирование жестокости и насилия вкупе со снижением уровня нравственного самосознания, коллапсом жизненных норм и ценностей, эскалацией агрессии представляет собой определенное условие для синтеза феноменального продукта деструктивного воздействия СМИ – массового сознания деструктивного типа. Синтез массового сознания деструктивного типа обусловливает и соответствующее ему девиантное поведение масс, которое угрожает целостности и сохранности общества как такового. Изменение этой тревожной тенденции требует и индивидуальных корректирующих усилий, и усилий группового действия, направленных на изменение функционирования всей системы СМИ.[51]

СМИ, постоянно тиражирующие негатив, агрессию, являются причиной того, что у аудитории (как уже упоминалось) возникает эффект «эмоционального выгорания», «усталость сострадать». Данная концепция была разработана тремя американскими социологами (К. Кинник, Д. Кругман, Г. Камерон) и явилась важным шагом в развитии исследований незапланированных эффектов массовой коммуникации.[52]

Опасность «усталости сострадать» заключается в том, что понижается порог чувствительности, и в сознании молодежи насилие начинает восприниматься как норма жизни. При этом сострадание жертвам такого насилия, а также наиболее социально уязвимым категориям населения притупляется.

Следовательно, появляется, с одной стороны, черствость, жестокость, неспособность к состраданию, склонность к агрессии,

[51] Павлова Е.Д. Информационный терроризм со стороны СМИ: целенаправленное формирование культа насилия // Экстремизм и СМИ... СПб.: Астерион, 2006. С. 126-127.

[52] Ясавеев И.Г. Конструирование социальных проблем средствами массовой коммуникации. Казань, 2004. С. 149.

с другой – повышается уровень тревожности, усиливается чувство собственной беззащитности, психологического дискомфорта, страха у многих людей. А у молодежи возникают трудности социализации. Для не вполне окрепшей психики информация об экстремистских инцидентах, проявлениях шовинизма, этнофобии может оказаться привлекательным примером, инструкцией к действию.[53]

Так, террористические организации осуществляют постоянный интернет-рекрутинг, в основном в среде подростков и молодежи, поэтому серьезной проблемой является то, как не допустить попадания молодежи в подобные террористические «сети».

Известно, что СМИ провоцируют этническую неприязнь, ксенофобные настроения, в чем проявляется еще одна дисфункция СМИ. Так, для формирования негативного отношения к субъекту чаще всего выступают нарочито грубые, вульгарные, стилистически сниженные слова и выражения, дискредитирующие личность и формирующие восприятие субъекта как подозрительного и нежелательного, вызывающего неприязнь.

В ход идут идеологемы уничтожения: «вытесняют», «заполняют», «наводняют», «нашествие», «засилье», «наглеют», «портят жизнь» и т.д. Это как будто бы уже не просто чужаки, а враги. Провокационный характер терминов, подобных этим: «лицо кавказской национальности», «цветное» население, иноземцы, приезжие и др. – демонстрирует «вредность» «не своих» и способствует нагнетанию межэтнической напряженности.[54]

По мнению Г. Кожевниковой, у многих российских журналистов существуют именно расистские установки, которые в стрессовой ситуации преодолели «барьеры приличия» и массово выплеснулись на страницы газет и на экраны телевидения. Язык и настроения вражды, экстремизм и заражение общества негативными эмоциями способны через бессознательное безнадежно поразить общество. По словам К. Юнга, ведь «никто не в силах защитить себя от такого влияния». Однако общество может че-

[53] Константинова Н.П. Экстремизм и СМИ: отражение в массовом сознании молодежи // Экстремизм и СМИ... СПб., 2006. С. 171.

[54] Мельник Г.С. Особенности освещения в СМИ проблемы иномерности // Экстремизм и СМИ... СПб., 2006. С. 48.

рез представителей законодательной власти инициировать принятие адекватных законов, способных регулировать деятельность СМИ, стоять на страже национальной (в том числе информационной) безопасности общества.[55]

Наибольшим воздействием на массовую аудиторию обладают аудиовизуальные масс-медиа. Создается особая среда, в которой объекты становятся реальными только в том случае, если они будут показаны по телевидению.[56]

Важнейшей современной особенностью деятельности экстремистских и террористических организаций является их активное использование виртуального пространства и современных информационно-коммуникативных технологий.

Все действия современных террористов рассчитаны на телевизионный или интернет-эффект. При его отсутствии стимул к проведению террористических акций пропадает.

В этом смысле терроризм, помимо общеизвестных точек зрения, понимается и как способ влияния на умонастроения, а его информационный фактор – это деструктивная роль СМИ в создании «рекламы» террористам и устрашения населения.

В ходе мониторинга Интернета МВД России в 2007 г. выявило 148 ресурсов, содержащих материалы террористической и экстремистской направленности.

На этих ресурсах работают квалифицированные психологи, способные в кратчайшие сроки составить психологический портрет человека, вступившего в общение на форуме, подобрать к нему соответствующий подход, определить возможные векторы применения данного человека в рамках экстремистской или террористической деятельности. Таким образом, огромный процент молодых людей, иногда даже не замечая этого, оказывается вовлеченным в противоправную и даже преступную деятельность,

[55] Березкина О.П. ТВ-технологии как средство формирования культуры насилия и управления массовым сознанием // Экстремизм и СМИ... СПб., 2006. С. 91.

[56] Белова Т.П., Щепеткова Е.В. Информационный фактор терроризма в оценках студентов г. Москвы и г. Иванова // Экстремизм и СМИ... СПб., 2006. С. 87.

пополняя ряды активистов террористических организаций или организаций экстремистского толка.[57]

Международные экстремистские и террористические организации в своей деятельности сегодня не только предъявляют требования государству и обществу, но и стремятся запугать общественное мнение, посеять атмосферу тревоги и неуверенности. И в этом невольными помощниками им часто становятся современные СМИ. Стремясь повысить свою популярность, СМИ зачастую становятся ретрансляторами террористических идей, не представляя до конца возможных последствий своих публикаций и их патогенного воздействия на массовую аудиторию.[58]

Правомерно говорить о дисфункции СМК. В.Е. Семенов, в частности, говорит о следующих: дезинформационная; агностическая (в противовес познавательно-просветительской функции); асоциализирующая; деморализующая; невротизирующе-антикатарсическая; эскапистско-наркотическая (в противоположность развлекательно-гедонистической функции); манипулятивно-внушающая; антиэстетическая; дезинтеграционно-отчуждающая.[59]

Для противодействия новейшим информационно-коммуникативным и манипулятивным технологиям, используемым экстремистскими и террористическими организациями, современное государство должно научиться использовать столь же эффективные методы ведения контрпропаганды в киберпространстве и

---

[57] Современный политический экстремизм: понятие, истоки, причины, идеология, проблемы, организации, практика, профилактика и противодействие / Рук. авт. колл. А.-Н.З. Дибиров, Г.К. Сафаралиев. Махачкала, 2009. С. 543.

[58] Современный политический экстремизм: понятие, истоки, причины, идеология, проблемы, организации, практика, профилактика и противодействие / Рук. авт. колл. А.-Н.З. Дибиров, Г.К. Сафаралиев. Махачкала, 2009. С. 534-535.

[59] Семенов В.Е. Дисфункциональность современных российских средств массовой коммуникации // Социальные коммуникации и информация: исследование, образование, практика. Тезисы межвузовской науч.-практ. конф. СПб., 1999. С. 33-34.

действовать не только в режиме реакции на действия экстремистов, но и на опережение.[60]

Многие страны вынуждены принимать специальные меры для защиты своих сограждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния, что составляет информационно-психологическую безопасность, под которой понимают состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий в инфосфере. Пользователи информационной среды должны иметь необходимые знания о возможных последствиях воздействия информации на психику. Необходимо усвоить правила техники информационно-психологической безопасности.[61]

Важным является обеспечение информационной безопасности России. Это необходимо для обеспечения социального здоровья людей, которое включает в себя не только физическое, психическое, духовное благополучие, но и информационное здоровье.[62]

Как полагает В.Е. Семенов, необходимо добиваться принятия Закона об информационно-психологической безопасности детей, подростков и молодежи от негативного воздействия СМИ и рекламы, Закона о нравственном контроле в сфере СМИ и рекламы (включая мобильную связь) в русле концепции «Доктрины информационной безопасности РФ».

Помимо юристов и педагогов, ведущую роль в этой духовной и политической борьбе за будущие поколения России должны занять психологи и социологи и, конечно, честные журналисты[63].

---

[60] Современный политический экстремизм: понятие, истоки, причины, идеология, проблемы, организации, практика, профилактика и противодействие / Рук. авт. колл. А.-Н.З. Дибиров, Г.К. Сафаралиев. Махачкала, 2009. С. 548.

[61] Ланцев И.А. Глобализм и проблемы информационно-психологической безопасности // Экстремизм и СМИ... СПб., 2006. С. 46.

[62] Томалинцев В.Н. Оценка российской молодежью современных средств массовой информации с позиций социального здоровья // Актуальные проблемы исследования социального здоровья молодежи. Ч. II: Информационно-аналитические материалы / Под ред. Р.А. Зобова. СПб., 2005. С. 46.

[63] Семенов В.Е. Современные российские СМИ как негативный фактор социализации молодежи // Экстремизм и СМИ... СПб., 2006. С. 86.

В борьбе с терроризмом необходимо использовать профилактические возможности СМИ. Необходима организация информационно-психологического противодействия террористическим и экстремистским организациям. Основная цель в информационной сфере – перехват стратегической инициативы в информационном противоборстве, нейтрализация каналов информационного воздействия и поддержки организованной преступности и терроризма как социально-политического явления, создание благоприятного информационно-пропагандистского фона для мероприятий по противодействию и нейтрализации организованной преступности, экстремизма и терроризма.[64]

Одной из основных целей экстремизма и терроризма является создание атмосферы общественной напряженности и страха посредством воздействия на массовую аудиторию.[65] Посредством СМИ экстремистские и террористические организации осуществляют вербовку новых членов, жертвами чего главным образом становится молодежь. Так, информационный аспект экстремизма и терроризма играет существенную негативную роль. Агрессия, культ насилия, интолерантные установки, тиражируемые СМИ, деструктивно влияют на общество, и в первую очередь на поколение молодых. Поэтому важное значение имеет использование профилактических возможностей средств массовой информации в снижении (а не нагнетании!) уровня межэтнической и межрелигиозной напряженности, агрессивности, социальной тревожности и страха, в воспитании молодежи и общества в целом в духе мира и конструктивного взаимодействия.[66]

---

[64] Рябинков А.Г., Рудаков А.Б. Информационно-психологические операции в борьбе с терроризмом и экстремизмом: Учебно-метод. пособие / Под общ. ред. Н.А. Гудкова. Домодедово, 2004. С. 23-25.

[65] Багаева А.А. Проблемы противодействия экстремизму и терроризму: историко-правовой аспект // Актуальные проблемы противодействия экстремизму. Материалы Международной научно-практической конференции. Северо-Кавказский горно-металлургический институт (государственный технологический университет). 2018. С. 276.

[66] Некрасова Е.В. Информационный аспект экстремизма и терроризма и деструктивные тенденции в СМИ // Вестник Российского университета дружбы народов. Серия: Социология. 2013. №6. С. 57-65.

ГЛАВА 3. ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

3.1. Правовое регулирование в сфере противодействия экстремизму в сети Интернет

Современное общество характеризуется высокой степенью развития информационно-коммуникационных технологий, но данный процесс имеет как положительные, так и отрицательные стороны. Так, информационные технологии и всемирная сеть Интернет облегчают обмен информацией гражданами и их объединениями в любое время, в любом месте, предоставляют возможности для интеллектуального развития, облегчают доступ к информации.

Однако в современных условиях информационные технологии широко используются экстремистскими и террористическими организациями в своей деятельности. Как средство распространения экстремистских материалов, сеть Интернет обладает определенными особенностями.

Так, он состоит из совокупности сетей, имеющих разное географическое расположение. А информация, которая размещается во всемирной паутине, становится доступной для неограниченного круга лиц, в разных частях света. Причем и лица, разместившие информацию, и лица, ею пользующиеся, могут сохранять анонимность.

Кроме того, в связи с отсутствием географических рамок, ограничение доступа к информации или блокировка сайта не избавляют от проблемы размещения такой информация в другом месте. Таким образом, на первый план выходят проблемы установления лиц, разместивших информацию экстремистской направленности в сети Интернет, а также установления владельца сайта, на котором были размещены данные материалы.

Для преступлений, совершаемых в сети Интернет, характерна высокая степень латентности, обусловленная применением механизмов обеспечения анонимности. Важно отметить, что

преступления экстремистской направленности, совершаемые в сети Интернет, зачастую имеют трансграничный характер, когда преступник и объект преступного посягательства находятся под юрисдикцией различных государств. Совершение преступного деяния, как правило, осуществляется дистанционно, причем часть таких действий может выполняться в автоматизированном режиме. Следы преступных действий в сети Интернет распределяются по множеству объектов и характеризуются отсутствием четко выраженного места преступления.

Кроме того, важно отметить нестандартность, сложность, многообразие и частоту обновления способов совершения преступлений и применяемых при этом специальных средств. Глобализация, сопровождающаяся формированием наднациональных институтов, обслуживающих интересы отдельных корпоративных групп и стран, разрушительно воздействует на государственный и общественный порядки, действующие в пределах конкретного национального пространства.[67]

Как известно, процесс глобализации активно используется организаторами и участниками экстремистских групп, которые принимают на вооружение новейшие информационно-коммуникационные технологии, делающие элементы их инфраструктуры менее уязвимыми для правоохранительных органов. В этих условиях происходит увеличение потенциала экстремистских организаций, действующих по принципу сетевой организации. Для данных организаций характерно наличие единых центров управления, информационно-коммуникативных каналов, а также использование автономного способа существования входящих в сообщество периферийных криминальных групп.[68]

Все это вызывает необходимость повышения внимания к особенностям глобального информационного общества, его системообразующим элементам, а также определенным коммуникационным структурам и явлениям, в совокупности детерминирующим

[67] Марченко М.Н. Глобализация и ее воздействие на современное национальное государство (методологический аспект) // Теоретико-методологические проблемы права. М., 2007. С. 65.

[68] Принципы борьбы с экстремизмом в сети и вне ее будут одинаковыми / Официальный сайт информационного портала SecurityLab.ru URL: http:// www.securitylab.ru/news.html (дата обращения: 25.05.2018 г.).

рост угроз информационного экстремизма, а также информации, способствующей возникновению феномена готовности к экстремистской деятельности.[69]

Экстремистские сообщества постоянно расширяют сферу своего информационного пространства, и в то же время прививают собственные установки широкой аудитории. Таким образом, информационный экстремизм может выступать в качестве подготовительного этапа для других, в том числе и крайних форм экстремизма, и формировать благоприятную среду для распространения экстремистских убеждений. Субъектом информационного экстремизма может стать как экстремистская группа, так и одно лицо. А основным методом информационного экстремизма выступает речевое воздействие.

В современных условиях возможности Всемирной сети по распространению информации и информационному воздействию практически равны возможностям традиционных средств массовой информации, в связи с чем возможности сети Интернет широко используются террористическими и экстремистскими формированиями в целях пропаганды национальной и религиозной нетерпимости.

Для России угрозу представляют ресурсы, направленные на осуществление информационной и финансовой поддержки террористических организаций, в том числе и международных. Такие ресурсы зачастую содержат призывы к совершению актов терроризма, а также пропагандируют религиозную нетерпимость, межнациональную рознь и сепаратизм.

В сети Интернет постоянно увеличивается количество сайтов, на которых распространяется информация, способствующая развитию экстремизма. Примечательно, что большая часть интернет-адресов таких сайтов зарегистрирована в других государствах. Справочные ресурсы, напрямую не призывающие к противоправной деятельности, но подразумевающие ее совершение, вызывают особую озабоченность правоохранительных органов России. Так как на таких ресурсах распространяется информация

[69] Мозговой В.Э. Информационный экстремизм в условиях глобализации и информатизации социума // Общество и право. 2015. №1 (51). С. 309-313. С. 309.

об изготовлении взрывчатых веществ, способах получения ядов, сборке самодельных взрывных устройств и т.д. Как правило, такие ресурсы недолговечны, часто меняют доменные имена и довольно многочисленны. Решению проблемы распространения экстремизма в сети Интернет будут способствовать унификация и совершенствование законодательства РФ в сфере распространения информации в телекоммуникационных сетях общего пользования.

Таким образом, в современных условиях, наряду с основными проявлениями экстремизма – политическим, национальным и религиозным, выделяют и информационный экстремизм. Образ экстремистских организаций, основывающихся на стремлении к национальному освобождению, действующих в рамках поставленных политических целей и финансируемых правительствами, начинает исчезать. На смену ему приходит информационный экстремизм, при котором один человек, являющийся носителем экстремистского сознания, в перспективе может нанести более масштабный урон, нежели более многочисленные экстремистские формирования.

Видится, что в настоящее время информационный экстремизм едва набирает силу, хотя, учитывая темпы развития современных информационно-коммуникационных технологий, расцвет этого вида экстремизма, к сожалению, может наступить очень скоро. Как справедливо отмечает А.В. Карягина, основным «оружием» информационного экстремизма является не нивелирование ценностей и символов существующего строя, а деформация важнейших коммуникационных связей[70] в целях развития хаоса в информационном обществе.

Кроме того, информационный экстремизм имеет еще одно проявление – связанное с информационным воздействием на широкий круг лиц при помощи средств массовой информации. Таким образом, пропагандистские призывы экстремистов могут стать убеждениями людей и способствовать совершению противоправных деяний, в том числе и совершаемых по мотивам рели-

[70] Карягина А.В. Информационный экстремизм в современном государственно-правовом пространстве //Философия права. 2010. №4. С. 105-107.

гиозной, расовой, половой и иной дискриминации. Это наносит большой вред нашей государственности, подрывает основы правовой культуры.

По нашему мнению, в современных условиях, характеризующихся развитием информационного общества и глобализацией, проблема информационного экстремизма стоит особенно остро. Во многом это связано с возможностью манипулирования индивидуальным и общественным сознанием, что в конечном итоге может привести к возникновению информационных войн. Все это выводит на новый уровень проблему обеспечения информационной безопасности.

Важно отметить, что в настоящее время происходит изменение структуры экстремистских группировок. Так, сегодня за счет развития новых информационно-коммуникационных технологий иерархическая структура экстремистских организаций, возглавляемых одним лицом, сменилась на сетевую, в рамках которой могут существовать и несколько лидеров. Все это усложняет работу по выявлению такого рода экстремистских организаций.

Особое место в деле противодействия экстремизму в сети Интернет занимает действенная правовая база.

В соответствии с Конституцией Российской Федерации в нашей стране не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства. Запрещается создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни.[71]

[71] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции РФ с внесенными поправками от 14.03.2020 опубликован на Официальном интернет-портале правовой информации [Электронный ресурс] // Режим доступа: http://www.pravo.gov.ru, 04.07.2020.

В соответствии со ст. 29 Конституции РСО-Алания запрещаются пропаганда и агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства. Ст. 12 запрещаются создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя или нарушение целостности Республики Северная Осетия – Алания, подрыв безопасности государства, создание на ее территории вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни.[72]

Под преступлениями экстремистской направленности в Уголовном кодексе Российской Федерации понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти, или вражды, либо по мотивам ненависти или вражды в отношении какой-либо социальной группы.

К данной категории преступлений относятся:

- публичные призывы к осуществлению экстремистской деятельности;

- создание экстремистского сообщества, то есть организованной группы лиц для подготовки или совершения преступлений экстремистской направленности, а равно руководство таким экстремистским сообществом, его частью или входящими в такое сообщество структурными подразделениями, а также создание объединения организаторов, руководителей или иных представителей частей или структурных подразделений такого сообщества в целях разработки планов и (или) условий для совершения преступлений экстремистской направленности;

- участие в экстремистском сообществе;

- организация деятельности общественного или религиозного объединения либо иной организации, в отношении которых судом принято вступившее в законную силу решение о ликвидации

[72] Конституция Республики Северная Осети – Алания (принята Верховным Советом Республики Северная Осетия 12.11.1994) (ред. от 04.03.2021) // Северная Осетия. 07.12.1994.

или запрете деятельности в связи с осуществлением экстремистской деятельности;

- участие в деятельности общественного или религиозного объединения либо иной организации, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

Подтверждением нарастающему напряжению в правоприменительной практике выступает и формирующаяся судебная практика, направленная на совершенствование подхода к вопросам понимания преступного деяния и наступления ответственности за его совершение. В рамках данного исследования интерес представляет анализ Постановления Пленума Верховного Суда РФ от 03.11.2016 №41 «О внесении изменений в постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 года №1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» и от 28 июня 2011 года №11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности».

Из положений, касающихся ст. 282 УК, важнейшим является разъяснение, устанавливающее, что возбуждение ненависти в том или ином проявлении – это не любые негативные высказывания, а именно призывы к противоправным действиям, и это необходимо учитывать при рассмотрении судами, следователями уголовных дел и квалификации деяний.

Другим важным разъяснением является позиция Верховного суда России по вопросу об оценке публикаций в сети Интернет, которая гласит, что при решении вопроса о направленности действий лица, разместившего какую-либо информацию либо выразившего свое отношение к ней в сети «Интернет» или иной информационно-телекоммуникационной сети, на возбуждение ненависти либо вражды, а равно унижение достоинства человека либо группы лиц следует исходить из совокупности всех обстоятельств содеянного и учитывать, в частности, контекст, форму и содержание размещенной информации, наличие

и содержание комментариев или иного выражения отношения к ней.[73]

Федеральным законом от 28.06.2014 года №179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» в ч. 2 ст. 280 УК РФ и в ч. 1 ст. 282 УК РФ были внесены изменения, предусматривающие в диспозиции указанных статей уголовную ответственность за призывы к осуществлению экстремистской деятельности, а также действия, направленные на возбуждение ненависти либо вражды, на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично или с использованием средств массовой информации либо информационно-коммуникационных сетей, в том числе сети Интернет.

Важно отметить, что до принятия указанного Закона конкретизации относительно информационно-коммуникационных сетей, в том числе сети Интернет, в уголовном законодательстве Российской Федерации не было. Ранее запрещалось распространение экстремистских призывов только в средствах массовой информации, к которым информационно-коммуникационные сети не относились.

Важно отметить, что за публичные высказывания, признанные судом экстремистскими, только в первой половине 2020 года было осуждено 132 человека, значительное число из которых были вынесены за высказывания, сделанные в онлайн-режиме.[74]

Таким образом, практика последних лет показывает, что борьба с проявлениями экстремизма за последние годы активно ста-

---

[73] Постановление Пленума Верховного Суда РФ от 03.11.2016 №41 «О внесении изменений в постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 года №1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» и от 28 июня 2011 года №11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности»// Российская газета. №259. 16.11.2016.

[74] Официальная статистика Судебного департамента Верховного суда в сфере борьбы с экстремизмом за первую половину 2020 года // Центр «Сова». 2020. 18 октября (https://www.sova-center.ru/racism-xenophobia/news/counteraction/2020/10/d43072/).

ла переходить из реального мира в онлайн. При этом на первый план выходят преступления, связанные с пропагандой идей национального, религиозного и расового превосходства посредством использования сети Интернет. Все это требует соответствующей реакции и со стороны правоохранительных органов.

Кроме того, в целях противодействия экстремизму используются следующие нормы Уголовного кодекса РФ, предусматривающие ответственность за преступления вне связи с экстремизмом, но нередко совершаемые или могущие совершаться и в экстремистских целях (ст. 105, 111, 112, 115, 116, 119, 126, 127, 136, 148-151, 156, 209, 210, 212-214, 215.2, 240, 241, 243, 244, 294-298, 317-319, 321, 322.1, 323, 329, 330 УК РФ), а также нормы, направленные против актов террористической деятельности как особых (специфических) проявлений экстремизма (ст. 205, 205.1, 205.2, 206, 208, 211, а также, согласно ст. 205.1 УК РФ, ст. 277, 278, 279, 360 УК РФ).[75]

В целях защиты прав и свобод человека и гражданина, основ конституционного строя, обеспечения целостности и безопасности Российской Федерации Федеральным законом от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности» определяются правовые и организационные основы противодействия экстремистской деятельности, устанавливается ответственность за ее осуществление.

31 июля 2020 г. Федеральным законом №299-ФЗ[76] было уточнено понятие экстремизма. Таким образом, в соответствии с внесенными изменениями под экстремизмом понимается:

- насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории Российской Федерации), за исключением делимитации, демаркации, ре-

[75] Башкатов Л.Н., Беляев А.Е., Игнатьев А.А., Изоитко С.И., Устинков А.В. Основные проблемы уголовно-правовой оценки проявлений экстремизма и терроризма // Право и безопасность. №3-4. 2007.

[76] Федеральный закон от 31.07.2020 №299-ФЗ «О внесении изменения в статью 1 Федерального закона «О противодействии экстремистской деятельности»» // Собрание законодательства РФ. 03.08.2020. №31 (часть I). Ст. 5058.

демаркации Государственной границы Российской Федерации с сопредельными государствами;

- публичное оправдание терроризма и иная террористическая деятельность;

- возбуждение социальной, расовой, национальной или религиозной розни;

- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;

- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;

- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

- совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации;

- использование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, за исключением случаев использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии;

- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.[77]

В соответствии с Федеральным законом «О противодействии экстремистской деятельности» Российской Федерации противодействие экстремистской деятельности осуществляется по следующим основным направлениям:

- принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности;

- выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.[78]

К профилактическим мерам относятся воспитательные, пропагандистские меры, направленные на предупреждение экстремистской деятельности.

---

[77] Федеральный закон от 25.07.2002 №114-ФЗ (ред. от 01.07.2021) «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 29.07.2002. №30. Ст. 3031.

[78] Федеральный закон от 25.07.2002 №114-ФЗ (ред. от 01.07.2021) «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 29.07.2002. №30. Ст. 3031.

Если имеются сведения о готовящихся противоправных действиях, содержащих признаки экстремистской деятельности, и при отсутствии оснований для привлечения к уголовной ответственности Генеральный прокурор Российской Федерации или его заместитель, либо подчиненный ему соответствующий прокурор или его заместитель направляет руководителю общественного или религиозного объединения, либо руководителю иной организации, а также другим соответствующим лицам предостережение в письменной форме о недопустимости такой деятельности с указанием конкретных оснований объявления предостережения.

Общественному или религиозному объединению либо иной организации может быть вынесено предупреждение в письменной форме о недопустимости такой деятельности с указанием конкретных оснований вынесения предупреждения, в том числе допущенных нарушений. Предупреждение общественному или религиозному объединению либо иной организации выносится Генеральным прокурором Российской Федерации или подчиненным ему соответствующим прокурором.

В Российской Федерации запрещаются распространение через средства массовой информации экстремистских материалов и осуществление ими экстремистской деятельности и использование сетей связи общего пользования для осуществления экстремистской деятельности; запрещаются распространение экстремистских материалов, а также их производство или хранение в целях распространения.

Ответственность, установленная законодательством Российской Федерации, предусмотрена для должностного лица, а также иного лица, состоящего на государственной или муниципальной службе, за высказывания о необходимости, допустимости, возможности или желательности осуществления экстремистской деятельности, сделанные публично, либо при исполнении должностных обязанностей, либо с указанием занимаемой должности, а равно непринятие должностным лицом в соответствии с его компетенцией мер по пресечению экстремистской деятельности. За осуществление экстремистской деятельности иностранные граждане и лица без гражданства, равно как и граждане Россий-

ской Федерации, несут уголовную, административную и гражданско-правовую ответственность в установленном законодательством Российской Федерации порядке.[79]

При проведении собраний, митингов, демонстраций, шествий и пикетирования запрещается иметь при себе оружие (за исключением тех местностей, где ношение холодного оружия является принадлежностью национального костюма), а также предметы, специально изготовленные или приспособленные для причинения вреда здоровью граждан или материального ущерба физическим и юридическим лицам; не допускается привлечение для участия в них экстремистских организаций, использование их символики или атрибутики, а также распространение экстремистских материалов.

В Доктрине информационной безопасности Российской Федерации в качестве одного из направлений обеспечения информационной безопасности в области государственной и общественной безопасности названо противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространению ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации.[80]

Основные цели обеспечения национальной безопасности определены Указом Президента РФ от 02.06.2021 №537 «О Стратегии национальной безопасности Российской Федерации». В данном документе указано, что «усиливающаяся нестабильность в мире, рост радикальных и экстремистских настроений могут привести к попыткам разрешить нарастающие межгосударственные противоречия за счет поиска внутренних и внешних врагов, к разрушению экономики, традиционных

[79] Федеральный закон от 25.07.2002 №114-ФЗ (ред. от 01.07.2021) «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 29.07.2002. №30. Ст. 3031.

[80] Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. №50. Ст. 7074.

ценностей и игнорированию основных прав и свобод человека».[81]

Несмотря на принимаемые меры, в Российской Федерации остается высоким уровень преступности в отдельных сферах. Совершается большое количество преступлений против собственности, в сфере использования водных, биологических и лесных ресурсов, в сфере жилищно-коммунального хозяйства, а также в кредитно-финансовой сфере. Растет число преступлений, совершаемых с использованием информационно-коммуникационных технологий. Дестабилизирующее влияние на общественно-политическую обстановку оказывают экстремистские проявления.[82]

29 мая 2020 года была утверждена Стратегия противодействия экстремизму в Российской Федерации до 2025 года, в которой отмечается что одним из основных источников угроз национальной безопасности Российской Федерации является экстремистская деятельность, осуществляемая националистическими, радикальными общественными, религиозными, этническими и иными организациями и объединениями, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной обстановки в стране.[83]

В Стратегии отмечается, что информационно-телекоммуникационные сети, включая сеть «Интернет», стали основным средством связи для экстремистских организаций, которые используются ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии.[84]

---

[81] Указ Президента РФ от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 05.07.2021. №27 (часть II). Ст. 5351.

[82] Указ Президента РФ от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 05.07.2021. №27 (часть II). Ст. 5351.

[83] Указ Президента РФ от 29.05.2020 №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. 01.06.2020. №22. Ст. 3475.

[84] Указ Президента РФ от 29.05.2020 №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. 01.06.2020. №22. Ст. 3475.

Важную роль в организации борьбы с терроризмом и экстремизмом играют нормативные правовые акты Президента и Правительства Российской Федерации, подзаконные нормативные правовые акты субъектов Российской Федерации, регламентирующие отдельные направления деятельности в области борьбы с терроризмом и экстремизмом, порядок межведомственного и международного взаимодействия в данной сфере.

Правовое регулирование интернет-контента, основывается на федеральных законах «О связи», «Об информации, информатизации и защите информации», «О средствах массовой информации» и др.

Особое значение среди перечисленных законов имеет ФЗ «Об информации, информационных технологиях и защите информации». Так, Закон устанавливает возможность ограничения Роскомнадзором доступа к информационным ресурсам, содержащим призывы к массовым беспорядкам, осуществлению экстремистской деятельности, на основе обращения Генерального прокурора Российской Федерации либо его заместителей.

Федеральный закон «О средствах массовой информации» установил, что использование СМИ с целью совершения преступных деяний, а также с целью 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, не допустимо.[85]

Наряду с уголовной ответственностью, за осуществление экстремистской деятельности российское законодательство предусматривает и административную ответственность.

Рассмотрим основные административные правонарушения, связанные с осуществлением экстремистской деятельности:

1) Статья 5.26 Кодекса РФ об административных правонарушениях (КоАП РФ) предусматривает ответственность за:

- воспрепятствование осуществлению права на свободу совести н свободу вероисповедания, в том числе принятию рели-

[85] Закон РФ от 27.12.1991 №2124-1 (ред. от 18.04.2018) «О средствах массовой информации» // Российская газета. №3. 08.02.1992.

гиозных или иных убеждений, или отказу от них, вступлению в религиозное объединение или выходу из него;

- умышленное публичное осквернение религиозной или богослужебной литературы, предметов религиозного почитания, знаков или эмблем мировоззренческой символики и атрибутики либо их порча или уничтожение.

2) Статья 5.38 «Нарушение законодательства о собраниях, митингах, демонстрациях, шествиях и пикетировании» предусматривает ответственность за:

- воспрепятствование организации или проведению собрания, митинга, демонстрации, шествия или пикетирования, проводимых в соответствии с законодательством Российской Федерации, либо участию в них, а равно принуждение к участию в них.

3) Статья 5.62 КоАП РФ устанавливает ответственность за дискриминацию, то есть нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его пола, расы, цвета кожи, национальности, языка, происхождения, имущественного, семейного, социального н должностного положения, возраста, места жительства, отношения к религии, убеждений, принадлежности или непринадлежности к общественным объединениям или каким-либо социальным группам. Нужно отметить, что те же деяния, совершенные с использованием служебного положения, будут влечь уголовную ответственность по статье 136 УК РФ.

4) Статья 13.15 КоАП РФ предусматривает административную ответственность за:

- распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года №114-ФЗ «О противодействии экстремистской деятельности», или об организации, включенной в опубликованный единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими,

без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена;

- публичное распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, а равно публичное осквернение символов воинской славы России, публичное оскорбление памяти защитников Отечества либо публичное унижение чести и достоинства ветерана Великой Отечественной войны, в том числе совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей (включая сеть «Интернет»);

- публичное распространение информации, отрицающей факты, установленные приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси, либо одобряющей преступления, установленные указанным приговором, а равно публичное распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, о ветеранах Великой Отечественной войны, в том числе совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей (включая сеть «Интернет»);

- распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств, незаконному изготовлению или переделке оружия, основных частей огнестрельного оружия, если эти действия не содержат признаков уголовно наказуемого деяния;

- производство либо выпуск продукции средства массовой информации, содержащей публичные призывы к осуществлению террористической деятельности, материалы, публично оправдывающие терроризм, или другие материалы, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, за исключением случаев, предусмотренных статьями 20.3, 20.3.1, 20.3.2 и 20.29 КоАП РФ.

5) Ст. 20.2.2 КоАП РФ «Организация массового одновременного пребывания и (или) передвижения граждан в общественных местах, повлекших нарушение общественного порядка» устанавливает ответственность за:

- организацию не являющегося публичным мероприятием массового одновременного пребывания и (или) передвижения граждан в общественных местах, публичные призывы к массовому одновременному пребыванию и (или) передвижению граждан в общественных местах либо участие в массовом одновременном пребывании и (или) передвижении граждан в общественных местах, если массовое одновременное пребывание и (или) передвижение граждан в общественных местах повлекли нарушение общественного порядка или санитарных норм и правил, нарушение функционирования и сохранности объектов жизнеобеспечения или связи либо причинение вреда зеленым насаждениям либо создали помехи движению пешеходов или транспортных средств либо доступу граждан к жилым помещениям или объектам транспортной или социальной инфраструктуры, за исключением случаев, предусмотренных частями 2 и 3 статьи 20.2.2 КоАП РФ, если эти действия не содержат уголовно наказуемого деяния;

- перечисленные выше действия, повлекшие причинение вреда здоровью человека или имуществу, если эти действия не содержат уголовно наказуемого деяния;

- перечисленные в первом пункте действия (бездействие), совершенные на территориях, непосредственно прилегающих к опасным производственным объектам или к иным объектам, эксплуатация которых требует соблюдения специальных правил техники безопасности, на путепроводах, железнодорожных магистралях, полосах отвода железных дорог, нефте-, газо- и продуктопроводов, высоковольтных линий электропередачи, в пограничной зоне, если отсутствует специальное разрешение уполномоченных на то пограничных органов, либо на территориях, непосредственно прилегающих к резиденциям Президента Российской Федерации, зданиям, занимаемым судами, или территориям и зданиям учреждений, исполняющих наказания в виде лишения свободы, если эти действия не содержат уголовно наказуемого деяния.

6) Статья 20.3 КоАП РФ устанавливает ответственность за:

- пропаганду либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами;

- изготовление или сбыт в целях пропаганды либо приобретение в целях сбыта или пропаганды нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами.

7) Статья 20.28 КоАП РФ предусматривает наказание за организацию деятельности общественного или религиозного объединения, в отношении которого действует имеющее законную силу решение о приостановлении его деятельности, а также участие в такой деятельности.

8) Статья 20.29 КоАП устанавливает ответственность за массовое распространение экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, а равно их производство либо хранение в целях массового распространения.[86]

Из перечисленных выше статей Кодекса РФ об административных правонарушениях чаще всего применяется статья 20.3 – пропаганда либо публичное демонстрирование нацистской атрибутики или символики. Осуществление данного правонарушения зачастую осуществляется в сети «Интернет», в социальных сетях. Российский исследователь А.В. Сигарев выделяет три группы случаев демонстрации такой символики:

1) когда эта символика используется сторонниками идей нацизма и имеет целью пропаганду данных идей, выражения

[86] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 01.09.2021) // Российская газета. №256. 31.12.2001.

приверженности лица этим идеям. В этой ситуации административная ответственность совершенно оправдана;

2) использование символики, схожей с нацистской (например, свастики), как древних религиозных символов, без цели пропаганды нацизма. На этом основании к административной ответственности неоднократно привлекались последователи различных неоязыческих культов, использующих такую символику в религиозных целях. На этом же основании некоторые религиозные организации были признаны экстремистскими;

3) демонстрация нацистской символики вообще без цели пропаганды каких-либо идей.[87]

Как видим, публичная демонстрация такой символики представлена разными целями и мотивами.

3.2. Профилактика борьбы с проявлениями экстремизма в сети Интернет в РСО-Алания

В условиях беспрецедентного распространения информационно-коммуникационных и цифровых технологий особо обострилась проблема роста экстремистских проявлений в сети «Интернет», и особенно в социальных сетях, которые зачастую используются как для распространения экстремистских материалов, демонстрации запрещенной символики, так и в других противоправных целях.

Как справедливо отмечают Е.И. Галяшина и В.Д. Никишин, «очевидно, что любые проявления экстремизма в глобальной телекоммуникационной сети Интернет с ее вирусоподобным распространением информации и охватом огромной по своим масштабам аудитории представляют реальную угрозу информационно-мировоззренческой безопасности граждан и нормальному функционированию органов государственной власти. Это требует адекватного реагирования, направленного на выявление и удаление из публичного виртуального пространства вредоносного контента, посредством признания его в судебном порядке экстре-

[87] Сигарев А.В. Правовое регулирование противодействия экстремизму: курс лекций. / А.В. Сигарев; СИУ-филиал РАНХиГС. Новосибирск: Изд-во СибАГС, 2015. С. 96-98.

мистским материалом и информацией, распространение которой запрещено в Российской Федерации».[88]

Реализуя общегосударственную политику по противодействию экстремизму, в том числе в сети Интернет, правоохранительными органами РСО-Алания реализуются мероприятия по противодействию проявлениям экстремизма. В соответствии с данными МВД в целом по стране, по итогам 2020 года, число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%[89].

Однако в 2021 году отмечается замедление темпов прироста количества зарегистрированных IT-преступлений. Если за первый квартал 2021 года их число возросло на 33,7%, то за семь месяцев текущего года этот показатель составил 15,7%. Две трети криминальных деяний в сфере высоких технологий совершены с использованием сети Интернет[90].

Приведенные данные свидетельствуют о широком распространении ИКТ, которые используются, в том числе, с целью совершения противоправных деяний экстремистского характера.

В соответствии со сведениями Информационно-аналитического портала правовой статистики Генеральной прокуратуры Российской Федерации, за 2020 год было зарегистрировано 883 преступления экстремистской направленности[91], данный показатель выше, чем в 2019 году (585), однако значительно ниже, чем в 2018 (1265) и 2017 (1521) годах. Однако в суд было передано в 2020 году 590 дел, в 2019 – 370, в 2018 – 958, в 2017 – 1109.

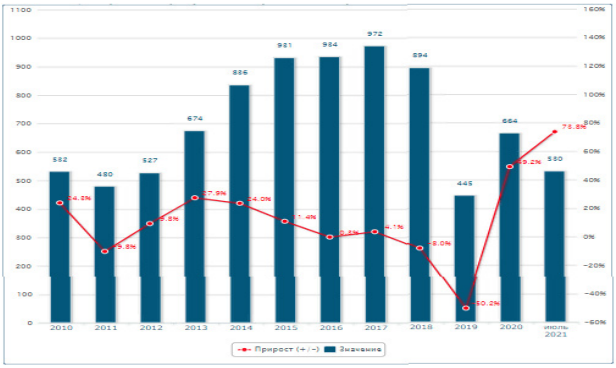
[88] Галяшина Е.И., Никишин В.Д. Особенности административных дел о признании информационных материалов экстремистскими и их экспертиза в аспекте безопасности интернет-коммуникации // Актуальные проблемы российского права. 2021. Т. 16. №7. С. 159-167.

[89] МВД РФ. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2020 года / [Электронный ресурс] // Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/22678184

[90] МВД РФ. Краткая характеристика состояния преступности в Российской Федерации за январь-июль 2021 года / [Электронный ресурс] // Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/25443630/

[91] Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации / [Электронный ресурс] // Режим доступа: http://crimestat.ru/offenses_chart

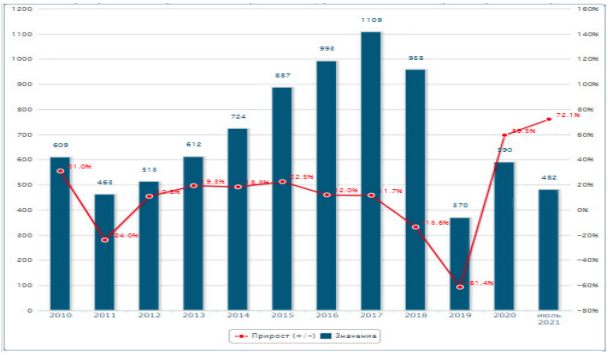
Выявлено лиц, совершивших преступления экстремистской направленности (рис. 2)



*По данным информационно-аналитического портала правовой статистики Генеральной прокуратуры Российской Федерации // Режим доступа: http://crimestat.ru/offenses_chart

Рисунок 1

Количество преступлений экстремистской направленности, уголовные дела о которых направлены в суд[92] (рис. 2)



*По данным информационно-аналитического портала правовой статистики Генеральной прокуратуры Российской Федерации // Режим доступа: http://crimestat.ru/offenses_chart

Рисунок 2

[92] Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации [Электронный ресурс] // Режим доступа: http://crimestat.ru/offenses_chart

Как показывают приведенные в графике данные, наибольшее количество преступлений экстремистской направленности (за последние 10 лет) было зарегистрировано (и рассмотрено в судах) в 2017 году, а наименьшее – в 2019 году.

Рост выявленных преступлений экстремистской направленности в 2017 году был связан:

- с решением задач, определенных для органов внутренних дел Стратегией противодействия экстремизму в Российской Федерации до 2025 года, план реализации которой утвержден Правительством Российской Федерации от 30 июня 2015 г. №4721п-П44;

- реализацией в рамках положений Указа Президента Российской Федерации от 7 мая 2012 г. №602 «Об обеспечении межнационального согласия» мероприятий, направленных на предупреждение межнациональных конфликтов, способных спровоцировать эскалацию напряженности и массовые беспорядки;

- осуществлением комплекса организационных и практических мероприятий, направленных на повышение эффективности противодействия всем видам экстремистских проявлений – от бытовой ксенофобии до сепаратизма и терроризма;

- реализацией Межведомственного плана по противодействию экстремизму на 2013-2018 годы;

- реализацией мероприятий по противодействию деятельности международных неправительственных организаций и фондов, направленных на поддержку носителей протестного потенциала.[93]

Сокращение преступлений экстремистской направленности в 2019 году, в том числе, связано и с частичной декриминализацией ч. 1 ст. 282 УК (возбуждение ненависти). При этом из 585 зарегистрированных преступлений 257 было совершено с использованием информационно-телекоммуникационных технологий.

Большинство преступных проявлений экстремизма в 2020 году связано с публичными призывами к осуществлению экс-

[93] Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор / Ю.М. Антонян, Д.А. Бражников, М.В. Гончарова и др. М.: ФГКУ «ВНИИ МВД России», 2018. С. 44.

тремистской деятельности (+34,9%, 367), значительная часть из которых совершена с использованием сети «Интернет» (339).[94] В общей структуре выявленных преступлений экстремистской направленности большая часть (500) выявлена сотрудниками органов внутренних дел.[95]

По количеству зарегистрированных преступлений экстремистской направленности по итогам 2020 года лидирует Республика Дагестан (69), Кемеровская область (40), г. Москва (36), Свердловская область (32), Республика Татарстан (24). В Республике Северная Осетия – Алания было зарегистрировано 5 преступлений, а в Ненецком и Чукотском автономных округах, а также в Республике Тыва не было зарегистрировано преступлений в исследуемой сфере.

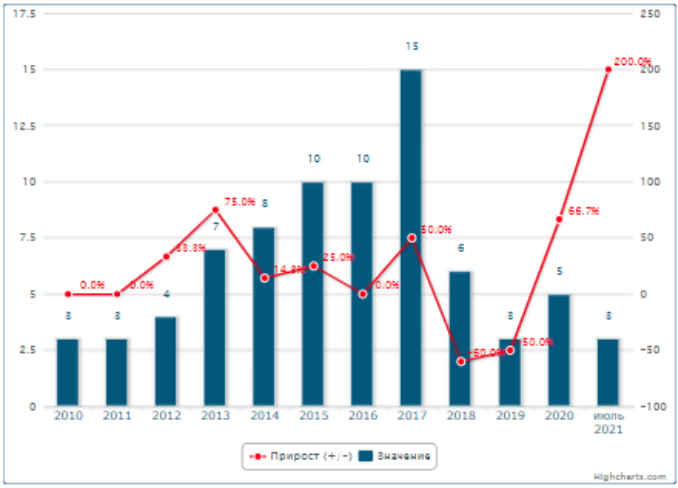
В 2020-2021 г. запрещена или приостановлена деятельность 14 экстремистских организаций: Религиозная группа «Алля-Аят»; Автономная некоммерческая организация «Благотворительный пансионат «Ак Умут» – «Светлая надежда»; Межрегиональное общественное объединение «Русская республика Русь»; Международное общественное движение «Арестантское уголовное единство»; Башкирская общественная организация «Башкорт»; Общественное объединение Комитет «Нация и свобода»; Общественное объединение «W.H.C.»; Хакасская региональная общественная организация духовного и физического самосовершенствования человека по Великому закону Фалунь «Фалунь Дафа»; Неформальное молодежное объединение футбольных фанатов «Иртыш Ultras»; Региональное общественное объединение «Русский Патриотический клуб – Новокузнецк/РПК»; Межрегиональное общественное движение «Сибирский державный союз»; Некоммерческая организация «Фонд борьбы с коррупцией»; Некоммерческая организация «Фонд

[94] Состояние преступности в России за январь-декабрь 2020 года. М., 2020. С. 8. [Электронный ресурс] // Режим доступа: https://media.mvd.ru/files/application/2041459

[95] Состояние преступности в России за январь-декабрь 2020 года. М., 2020. С. 20. [Электронный ресурс] // Режим доступа: https://media.mvd.ru/files/application/2041459

защиты прав граждан»; Общественное движение «Штабы Навального».[96]

Динамика зарегистрированных преступлений экстремистской направленности, совершенных на территории РСО-Алания, представлена в графике (рис. 3)



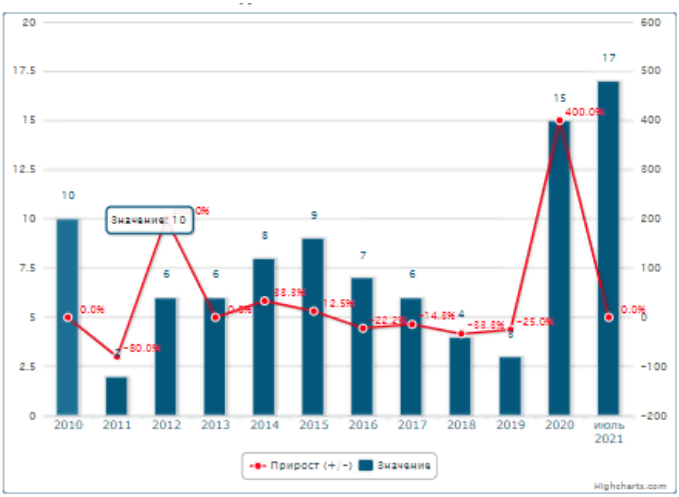
*По данным информационно-аналитического портала правовой статистики Генеральной прокуратуры Российской Федерации // Режим доступа: http://crimestat.ru/offenses_chart

Рисунок 3

Как показывают приведенные в графике данные, так же как и на общегосударственном уровне, за последние 10 лет наибольшее количество преступлений было зарегистрировано в 2017 году, а в 2020 году наблюдается рост по сравнению с 2019 годом.

Динамика количества выявленных лиц, совершивших преступления экстремистской направленности на территории РСО-Алания, представлена в графике (рис. 4).

[96] Перечень общественных объединений и религиозных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности». / [Электронный ресурс] // Режим доступа: https://minjust.gov.ru/ru/documents/7822/



*По данным информационно-аналитического портала правовой статистики Генеральной прокуратуры Российской Федерации // Режим доступа:http://crimestat.ru/regions_chart_total

Рисунок 4

Приведенные в графике данные свидетельствуют о росте количества выявленных лиц, совершивших преступления экстремистской направленности на территории РСО-Алания. Во многом это связано с эффективной работой правоохранительных органов на территории республики.

Как отметил министр внутренних дел в своем выступлении перед парламентом республики, сотрудниками МВД решались задачи, направленные на предупреждение, выявление и пресечение угрозообразующих факторов, обусловленных распространением радикальной идеологии, националистической пропаганды и иных экстремистских проявлений, в том числе в информационно-телекоммуникационной сети «Интернет». В 2020 году сотрудниками североосетинской полиции выявлено и заблокировано свыше 900 интернет-ресурсов, пропагандирующих экстремистскую идеологию[97].

[97] Михаил Скоков выступил перед Парламентом республики // https://15.xn--b1aew.xn--p1ai/news/item/23589143/

Социальные сети, блоги и пространства для комментариев – все это платформы для выражения мнений, публичного выступления или пропаганды. Все чаще эти каналы используются для распространения экстремистских взглядов или для вербовки членов в экстремистские группы.

В сети «Интернет» экстремистские воззрения распространяются гораздо быстрее, чем в физическом мире. Это объясняется, в частности, тем, что сеть «Интернет» позволяет каждому публично выражать свои идеи, не раскрывая свою личность. Кроме того, в сети «Интернет» очень легко создать фальшивую личность, поддельные новости, осуществлять различные манипуляции.

В последние годы в сети «Интернет» стали широко распространяться всевозможные виды экстремистской деятельности. В частности, социальные сети используются экстремистскими группами в качестве пропагандистских инструментов для привлечения, радикализации и мобилизации новых членов.

Однако лишь незначительная доля проявлений экстремизма выявляется в рамках инициативного реагирования граждан. С учетом специфики, выявить все случаи проявлений экстремизма не представляется возможным. По этой причине организационно-правовые основы противодействия экстремизму в сети «Интернет» должны постоянно совершенствоваться.

Исследования показали, что особенно молодые люди в поисках идентичности и ориентации становятся мишенью радикальных формирований.[98]

[98] Профилактика экстремизма в молодежной среде: информационно-методический сборник. Иркутск, 2020 г. 131 с.; Профилактика экстремизма в молодежной среде: учебное пособие для вузов / А.В. Мартыненко [и др.]; под общ. ред. А.В. Мартыненко. Москва: Издательство Юрайт, 2020. 221 с. (Высшее образование). – ISBN 978-5-534-04849-0. – Текст: электронный // ЭБС Юрайт [сайт]. – URL: https://urait.ru/bcode/454111; Бааль Н.Б. Молодежные экстремистские организации в постсоветской России // История государства и права. 2007. №11. С. 26; Социокультурные особенности молодежного экстремизма: монография / А.Р. Тузиков, Р.И. Зинурова, Э.Б. Гаязова, С.А. Алексеев. Казань: Казанский национальный исследовательский технологический университет, 2015. 188 с. – ISBN 978-5-7882-1863-2. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/63999.html; Кудрин В.С. Молодежный экстремизм: причины возникновения, технологии предупреждения. Учебное посо-

В этом отношении профилактика экстремизма в молодежной среде ведется в следующих областях:

- взаимодействие образовательных учреждений с родителями;

- профессиональное развитие профессорско-преподавательского состава по этому вопросу;

- включение в образовательную программу конкретных тем, связанных с профилактикой экстремизма;

- введение в образовательные программы предметов, связанных с нравственным воспитанием детей и молодежи;

- непрерывный мониторинг уровня толерантности в обществе, и особенно среди молодежи;

- вовлечение молодежи в культурные мероприятия;

- реализация потребности в самореализации и самовыражении;

- организация досуга учащихся;

- персонификация пользователей при регистрации в социальных сетях и т.д.

Профилактике распространения экстремизма в интернет-пространстве будет способствовать формирование в рамках семьи, научных, образовательных и других учреждений критического мышления у молодежи (не верить всему, что написано и показано в Интернете, и подвергать сомнению онлайн-контент); проверка фактов и источников (одна и та же тема или событие может сообщаться в разных источниках по-разному); проверка подлинности изображений и видео, так как современная техника позволяет легко подделывать изображения и видео.

Федеральный закон от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности» устанавливает следующие основные меры противодействия исследуемому явлению:

- принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявле-

---

бие / В.С. Кудрин, А.И. Юдина. Кемерово: Кемеровский государственный институт культуры, 2016. 160 с. – ISBN 978-5-8154-0326-0. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/55796.html; Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности // Юридический мир. 2008. №6. С. 26.

ние и последующее устранение причин и условий, способствующих осуществлению указанной деятельности;

- выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

По нашему мнению, профилактика правонарушений экстремистской направленности во многом зависит от эффективности осуществляемой политики государства в этой сфере. Являясь актором, который несет основную ответственность за противодействие экстремистским проявлениям, оно направляет вектор развития антиэкстремистского законодательства, правоприменительной практики, сотрудничества.

Однако имеющийся потенциал правового противодействия экстремизму не всегда используется в полной мере в силу недостаточной эффективности правоприменительной деятельности, а также в связи с существующими пробелами в законодательном регулировании данного вопроса, что требует дальнейшего совершенствования этих мер.[99] Качественно разработанная нормативно-правовая база, учитывающая специфику цифровизации, является важнейшим условием эффективности предупреждения преступлений.[100]

Особую роль в деле предупреждения экстремизма может и должна сыграть общегосударственная идеология, направленная на сплочение общества и государства, на достижение общественно полезных целей, одной из которых будет являться нетерпимость со стороны всех членов общества к преступному поведению в целом и к экстремизму в частности.[101]

Особую роль в деле профилактики правонарушений экстремистского характера имеют реализуемые в регионах программы. Так, в РСО-Алания реализуется государственная программа Республики Северная Осетия – Алания «Развитие межнациональ-

[99] Певцова Е.А. Экстремистские проявления в поведении молодежи в период правовых реформ и кризисных явлений в государстве: проблемы профилактики // Российская юстиция. 2009. №7. С. 13-22.

[100] Жалинский А.Э. Условия эффективности профилактики преступлений. М., 1978. С. 47.

[101] Петряние А.В. Противодействие преступлениям экстремистской направленности: уголовно-правовой и криминологический аспекты. Дисс. … д.ю.н. М., 2014. С. 380.

ных отношений в Республике Северная Осетия – Алания» на 2019-2025 годы, одной из целей которой выступает профилактика экстремистских проявлений и идеологии терроризма. В программе отмечается, что экстремизм во всех его проявлениях ведет к попранию прав и свобод граждан, подрывает общественную безопасность, государственную целостность и международный авторитет России, создает реальную угрозу основам конституционного строя, межнациональному и межконфессиональному миру.

В этой связи необходима система мер по нейтрализации причин и условий, способствующих возникновению религиозного экстремизма, этносепаратизма и их последствий – социальных, межэтнических и религиозных конфликтов. Важнейшее место в борьбе с экстремизмом занимает предупреждение его проявлений.

Решение поставленных задач обеспечивается соответствующими органами государственной власти во взаимодействии с общественными и религиозными институтами. Необходимы организация и проведение разъяснительной работы среди населения, скоординированные совместные усилия представителей всех ветвей власти, правоохранительных органов и самого населения по устранению причин, порождающих экстремистские проявления.

Важно проведение превентивной политики в сфере борьбы с экстремизмом. Профилактика должна осуществляться на допреступных стадиях развития негативных процессов, то есть на этапах, когда формируется мотивация противоправного поведения. Необходимо полностью задействовать не только возможности всех органов государственной власти, участвующих в рамках своей компетенции в предупреждении экстремистской деятельности, но также и негосударственных структур. Для противодействия экстремизму необходима систематическая разъяснительная работа среди населения с привлечением специалистов в области теологии, обществоведения, психологии, юриспруденции, средств массовой информации.[102]

[102] Постановление Правительства Республики Северная Осетия – Алания от 27.11.2018 №375 «О Государственной программе Республики Северная Осетия – Алания «Развитие межнациональных отношений в Республике Северная Осетия – Алания» на 2019-2025 годы» // Официальный интернет-портал правовой информации. / [Электронный ресурс] // Режим доступа: http://pravo.gov.ru

Важное место в деле профилактики правонарушений экстремистского характера играют органы Министерства внутренних дел России (согласно приведенным ранее данным, именно сотрудниками МВД России было привлечено к ответственности подавляющее число правонарушителей), органы Прокуратуры РФ.

В республике реализуется комплекс мероприятий по противодействию распространению экстремистских проявлений в сети Интернет. Вместе с тем, имеют место сферы деятельности, где взаимодействие правоохранительных органов, а также их реагирование остается недостаточным. Количество выявляемых нарушений законодательства в сфере противодействия терроризму и экстремистской деятельности, в том числе в органах местного самоуправления, остается высоким.

Как уже было отмечено выше, воздействию радикальных идей подвержены более всего молодые люди. Поэтому вопросы профилактики и противодействия идеологии терроризма в молодежной среде являются чрезвычайно важными.

Естественно, большую часть информации молодежь получает именно через социальные сети. В современном информационном потоке молодому поколению сложнее всего найти правильный источник, из которого можно получать информацию. За информацией необходимо следить, чтобы успеть вовремя среагировать на опасные сведения.

В этой связи, особо хочется отметить деятельность Прокуратуры РСО-Алания. Так, например, в июле 2021 года по постановлению прокуратуры Моздокского района Республики Северная Осетия – Алания местный житель привлечен к ответственности за распространение экстремистских материалов. Прокуратура Моздокского района Республики Северная Осетия – Алания в рамках работы межведомственной рабочей группы совместно с территориальным отделом ЦПЭ МВД по РСО-Алания провела проверку соблюдения законодательства о противодействии экстремистской деятельности.

Установлено, что 37-летний местный житель на своей странице в социальной сети «В Контакте» разместил видеоролик, признанный экстремистским и запрещенным на территории Российской Федерации. Указанные обстоятельства послужили основани-

ем для возбуждения прокуратурой района в отношении мужчины дела об административном правонарушении, предусмотренном ст. 20.29 КоАП РФ (производство и распространение экстремистских материалов). Постановление прокуратуры рассмотрено и удовлетворено, виновный привлечен к административной ответственности в виде штрафа, запрещённый материал удален.[103]

С целью устранения выявленных нарушений и защиты прав несовершеннолетних, прокурор Правобережного района внес представления в адрес главы АМС района и руководителей образовательных учреждений, с постановкой вопроса о привлечении виновных к дисциплинарной ответственности.[104]

Также в апреле 2021 г. Прокуратура Республики Северная Осетия – Алания совместно с Центром по противодействию экстремизму МВД республики провела проверку соблюдения законодательства о противодействии экстремистской деятельности. Установлено, что 25-летний житель Владикавказа в апреле 2021 года на страницах одной из публичных групп социальной сети «В Контакте» оставил комментарии, имеющие явно оскорбительный унизительный характер по отношению к группе лиц по признакам расы, национальности, языка и происхождения.

Указанные обстоятельства послужили основанием для возбуждения прокуратурой республики в отношении «комментатора» дела об административном правонарушении, предусмотренном ст. 20.3.1 КоАП РФ (действия, направленные на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть «Интернет», если эти действия не содержат уголовно наказуемого деяния, влекут административную ответственность). Постановление прокуратуры рассмотрено судом, ви-

[103] По постановлению прокуратуры Моздокского района Республики Северная Осетия – Алания местный житель привлечен к ответственности за распространение экстремистских материалов. https://epp.genproc.gov.ru/ru/web/proc_15/mass-media/news?item=63604098

[104] http://www.procuror-osetia.ru/news/item/5725/

новный привлечен к административной ответственности в виде штрафа в размере 10 тысяч рублей.[105]

Кроме того, важное место в деле противодействия экстремизму в сети Интернет на территории республики занимает Управление Следственного комитета. Следственным управлением в рамках установленных полномочий проводится регулярная работа, направленная на противодействие экстремистской и террористической деятельности. В этой связи вопросы совершенствования межведомственного сотрудничества в области профилактики и противодействия экстремистской деятельности, выявления и пресечения деятельности лиц, осуществляющих вербовку новых участников бандподполья, выявление лиц, участвующих в вооруженных конфликтах на территории иностранных государств, являются предметом регулярного обсуждения и взаимодействия правоохранительных ведомств, органов власти и управления республики.

Данная работа в следственном управлении осуществляется в рамках деятельности межведомственной координационно-аналитической следственно-оперативной группы по раскрытию и расследованию преступлений террористического характера и иных преступлений, вызвавших общественный резонанс в Республике Северная Осетия – Алания.

В соответствии с Приказом Председателя Следственного комитета Российской Федерации от 12.07.2011 №109 «О мерах по противодействию экстремистской деятельности» на базе Межведомственной группы продолжает свою деятельность, постоянно действующая контрольно-аналитическая группа по противодействию экстремизму.

В рамках работы контрольно-аналитической группы и координации деятельности по противодействию экстремизму анализируется состояние преступлений, связанных с экстремистскими проявлениями в Республике Северная Осетия – Алания, определяются и вырабатываются меры, направленные на предупрежде-

[105] По постановлению прокуратуры Республики Северная Осетия – Алания местный житель привлечен к административной ответственности за оскорбительные комментарии в социальной сети / [Электронный ресурс] // Режим доступа: https://vladikavkaz.bezformata.com/listnews/prokuraturi-respubliki-severnaya-osetiya/94756668/

ние, пресечение и борьбу с подобными фактами. Осуществляется контроль над рассмотрением сообщений и расследованием уголовных дел экстремистской направленности.

Наряду с реализуемыми полномочиями по осуществлению уголовного преследования в пределах установленной компетенции, следственным управлением совместно с другими правоохранительными органами (ЦПЭ МВД по РСО-Алания и УФСБ РФ по РСО-Алания) продолжает осуществляться и иная работа, направленная прежде всего на профилактику преступлений анализируемой категории, а также минимизацию последствий её проявлений.

Другим направлением деятельности правоохранительных органов республики является работа по выявлению и пресечению деятельности на территории субъекта общественных организаций, фондов, движений, объединений, в том числе и религиозных, функционирование которых может быть связано с финансированием членов экстремистских организаций, незаконных вооруженных формирований и бандподполья, как на территории РСО-Алания, так и в других сопредельных субъектах Северо-Кавказского региона, а также вербовки жителей республики в ряды участников незаконных вооруженных формирований.

В целях превентивного выявления лиц, склонных к провокационным высказываниям и призывам, склонению жителей РСО-Алания к участию в незаконных вооруженных формированиях, в следственном управлении продолжена деятельность по ежедневному мониторингу сети Интернет и СМИ, куда входят федеральные и региональные телеканалы, печатные издания, а также радио и телеэфир. Оперативными службами республики в целях недопущения развития и распространения религиозно-экстремистской пропаганды на постоянной основе проводятся профилактические мероприятия по отслеживанию обстановки, складывающейся как в общей межконфессиональной среде, так и в конкретных религиозных общинах.

По словам начальника отдела по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму прокуратуры республики Александра Коптева, «работниками прокуратуры

в круглосуточном режиме обеспечивается мониторинг средств массовой информации и сети «Интернет» на предмет выявления материалов с признаками, создающими благоприятную почву для террористических и экстремистских проявлений. В результате регулярного мониторинга прокурорами выявлены факты размещения в Сети вредоносных материалов, по которым в суды направлены 226 исковых заявлений, в том числе 4 – о признании их экстремистскими.

На основании подготовленных прокуратурой республики материалов Генеральной прокуратурой Российской Федерации внесены 14 требований о блокировке 226 ресурсов о фейках о коронавирусе и призывах к митингам. Выявлены также печатные издания и видеоролики экстремистской направленности, по которым прокуратура также обратилась с исками в суд. По постановлениям прокуроров 29 лиц привлечены к административной ответственности за правонарушения экстремистской направленности. Положительный результат приносит работа по ограничению доступа к вредоносным интернет-ресурсам во внесудебном порядке, которая также показала свою эффективность»[106].

Следует отметить, что работа, направленная на противодействие проявлениям экстремизма и терроризма, продолжает осуществляться различными органами государственной власти в тесном взаимодействии с заинтересованными правоохранительными органами республики.

Большую работу по профилактике экстремистских проявлений в Республике Северная Осетия – Алания осуществляет Министерство РСО-Алания по вопросам национальных отношений, которое осуществляет профилактику на допреступных стадиях развития негативных процессов, то есть на этапах, когда формируется мотивация противоправного поведения.

Министерство Республики Северная Осетия – Алания по вопросам национальных отношений является ответственным исполнителем государственной программы Республики Северная Осетия – Алания «Развитие межнациональных отношений в Республике Северная Осетия – Алания» на 2019-2025 годы.

В рамках реализации подпрограммы 2 «Профилактика экс-

[106] Гацоева Н. Угрозы в сети и наяву // Северная Осетия. 23.03.2021.

тремизма на национальной, религиозной почве и идеологии терроризма в Республике Северная Осетия – Алания» предусматривается реализация следующих основных направлений:

- мониторинг и анализ межнациональных, этноконфессиональных отношений, политических, социально-экономических и иных процессов, оказывающих влияние на ситуацию в сфере противодействия терроризму и профилактики этнического и религиозного экстремизма;

- реализация мер по профилактике и предупреждению попыток разжигания национальной и религиозной розни, ненависти либо вражды;

- мероприятия общей профилактики экстремистских и ксенофобских проявлений;

- информационно-пропагандистское сопровождение профилактики экстремизма и терроризма.

Министерством проводится систематическая разъяснительная работа среди населения с привлечением специалистов в области теологии, обществоведения, психологии, юриспруденции, средств массовой информации; обучающие семинары-совещания для работников органов муниципальной и исполнительной власти республики.

Вовлечение населения, в том числе и молодежи, в реализацию мероприятий подпрограммы – эффективное средство профилактики экстремистских проявлений.

Сотрудниками Министерства проводятся встречи с учащимися высших и средних образовательных учреждений с целью повышения правовой культуры несовершеннолетних по вопросам предупреждения межэтнической напряженности, уголовной и административной ответственности за экстремистские проявления. В различных районах РСО-Алания ведётся информационно-профилактическая работа с молодёжью, прежде всего о правильном поведении в интернет-пространстве, об анализе поступающей информации в новостную ленту личного аккаунта в социальных сетях. Обращают также внимание на информацию, самостоятельно публикуемую молодыми пользователями.

В деле профилактики экстремизма, в том числе в сети «Интернет», особо следует отметить проводимые на территории

РСО-Алания мероприятия по общественному обсуждению проблематики экстремизма и терроризма, привлечения к данному процессу молодежи.

Так, например, в ноябре 2020 года Министерством РСО-Алания по вопросам национальных отношений, Домом дружбы народов РСО-Алания совместно с Центром социальных инноваций, компетенций и добровольчества был проведен круглый стол «Мы разные, но равные». В работе круглого стола приняли участие представители прокуратуры, Центра противодействия экстремизму и терроризму МВД по РСО-Алания, научного сообщества и молодежи.

В июле 2021 года во Владикавказе состоялась организованная Министерством РСО-Алания по вопросам национальных отношений Межрегиональная научно-практическая конференция «Этноконфессиональные аспекты формирования радикального мышления и экстремистской идеологии в молодёжной среде». Участники заслушали доклады, посвящённые формированию гражданской идентичности в молодёжной среде в СКФО, путям преодоления кризиса в этнокультурном развитии Северного Кавказа, молодежному экстремизму, роли институтов гражданского общества в формировании антитеррористических ценностей, СМИ – как инструменту борьбы с формированием радикального мышления и экстремистской идеологии коммуникаций РСО-Алания, государственно-конфессиональным отношениям, межрелигиозной консолидации и духовному образованию.

Обсудили организационно-управленческие практики противодействия экстремистской идеологии в сети Интернет, социальные факторы международного терроризма, профилактические меры в районах республики, проблемы нормативно-правовой регламентации профилактики экстремизма в сфере межэтнических и межрелигиозных отношений, религиозные конфликты публичных лиц в РСО-Алания как катализатор радикализации общества, информационную безопасность, влияние миграционного фактора на функционирование системы безопасности и многое другое.

Такого рода конференции уже стали регулярными благодаря организатору – Министерству РСО-Алания по вопросам национальных отношений.

На современном этапе важное значение приобретает подготовка специалистов и повышение квалификации в вопросах профилактики экстремизма и терроризма в интернет-пространстве. Что касается подготовки специалистов, то эта работа пока не налажена на должном уровне. Однако профилактическая работа по борьбе с распространением идей экстремизма и терроризма в социальных сетях проводится во многих вузах РСО-Алания.

Из вышесказанного видно, что в РСО-Алания проводится разносторонняя работа по профилактике идеологии экстремизма и терроризма в сети Интернет, духовному и патриотическому воспитанию молодежи. Но такая серьёзная угроза, как мировой терроризм и распространение его идеологии в интернет-пространстве, заставляет всё человечество быть предельно бдительными.

3.3. Проблемы борьбы с экстремизмом в сети Интернет на территории РСО-Алания

Как было показано в предыдущих параграфах, в нашей стране сформирована система законодательства о противодействии экстремизму, включающая в себя несколько десятков нормативно-правовых актов во главе с базовым Федеральным законом от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности». А в документах политико-правового характера определены стратегические направления государственной политики в этой сфере. Действует целая система государственных органов по противодействию экстремизму.

Однако на современном этапе развития общества международная информационно-коммуникационная сеть Интернет активно используется для размещения и распространения экстремистских материалов. Проблема является весьма актуальной и для Российской Федерации и ее регионов. Используя глобальную сеть Интернет и возможности компьютерной коммуникации, идеологи экстремистских движений и групп активно воздействуют на сознание граждан, и в первую очередь молодежи. В результате в последние годы происходит обострение проблемы экстремизма,

которая в настоящее время выделена в качестве одной из основных угроз национальной безопасности России[107].

Особую остроту проблематика противодействия экстремизму имеет для РСО-Алания как одного из наиболее проблемных регионов, находящегося в силу своего геополитического положения в эпицентре этнополитических, этноконфессиональных и социально-экономических процессов на Северном Кавказе.

Исследователи выделяют существование ряда проблем технического характера по противодействию экстремизму и терроризму в информационном пространстве:

- установление лица, разместившего в сети экстремистский или террористический материал. Современные технологии беспроводного доступа в сеть (например, Wi-Fi), имеющиеся в свободной продаже сетевые платы с динамическим IP-адресом и т. п. фактически исключают обнаружение такого лица;

- идентификация лица как автора или издателя экстремистского или террористического материала, а не просто как владельца средства вычислительной техники, посредством которого в сети был размещен материал.[108]

Кроме того, можно констатировать существование и других проблем в исследуемой сфере. Так, в ежегодных докладах о деятельности Уполномоченного по правам человека в РФ, материалах других правозащитных институтов приводятся многочисленные факты, когда противодействие экстремизму зачастую приводит к нарушениям конституционных прав и свобод человека и гражданина.

Однако имеется другая тенденция, связанная с тем, что в сознании граждан еще не сформировалась политико-правовая культура, позволяющая отличить законную общественно-политическую активность от проявлений экстремизма.

В этой связи, само понятие экстремизма в российском законо-

[107] Троегубов Ю.Н. Проблемы противодействия экстремизму в сети интернет // Гуманитарный вектор. Серия: История, политология. 2014. №3 (39). С. 144.

[108] Функционально возможные инструментальные средства противодействия распространению идей экстремизма и терроризма в сети Интернет на территории РФ. [Электронный ресурс] // Режим доступа: http://www.bibliofond.ru/view

дательстве, очевидно, требует уточнения. Следует отметить, что данная проблема также характерна для многих государств, которые реализуют политику в сфере противодействия экстремизму и терроризму.

В числе проблемных моментов необходимо назвать несовершенство нормативно-правовой базы РФ в сфере противодействия экстремизму в сети Интернет. В этой связи В.В. Баранов и Е.А. Исаев справедливо отмечают, что законодательство не предполагает детальной регламентации специальных мер государственного принуждения в отношении субъектов, использующих сети связи в преступных целях. Делается лишь отсылка к общим нормам Закона о противодействии экстремистской деятельности и законодательства в области связи.[109]

По нашему мнению, существует необходимость проведения кропотливой работы по приведению в соответствие Кодекса РФ об административных правонарушениях, Уголовного кодекса РФ и Федерального закона «О противодействии экстремистской деятельности» таким образом, чтобы каждое проявление экстремизма влекло административную или уголовную ответственность.

В числе проблемных моментов следует выделить также отсутствие единой методологии проведения экспертизы экстремистских материалов. Особенно важно выработать критерии отнесения религиозных текстов к экстремистским материалам.

По нашему мнению, недопустимым является признание канонических религиозных текстов или трудов богословов по формальному признаку пропаганды «религиозного превосходства» экстремистскими материалами. Проведение качественного экспертного исследования и надлежащей оценки смысловой направленности материалов специалистами, профессионально владеющими знаниями в области социальной психологии, лингвистики, психолингвистики, является одной из эффективных мер в сфере противодействия экстремизму, в том числе в сети Интернет.

Однако в процессе расследования уголовных дел данной категории возникают коллизионные моменты, связанные с тем, что не

[109] Баранов В.В., Исаев Е.А. О правовом регулировании деятельности органов внутренних дел по противодействию экстремистским проявлениям в информационном пространстве // 2020. №2 (54). С. 14-20.

позволяет сформировать единообразную практику в этой части. Кроме того, нередко заключения по одному и тому же материалу носят взаимоисключающий характер.

В качестве еще одной проблемы можно выделить длительный период проведения психолого-лингвистических исследований и судебных экспертиз, которые, как правило, проводятся больше 6 месяцев. Несомненно, это отрицательно сказывается на качестве следствия.

В деятельности государственных органов по противодействию экстремизму недопустим формализм, стремление к достижению количественных показателей любой ценой, а также подмена реальной деятельности всевозможными планами, программами, концепциями и отчетами.[110]

Для повышения эффективности работы в сфере противодействия экстремизму в Интернете необходимо обеспечить системный мониторинг средств массовой информации, технических каналов связи на предмет выявления провайдеров и отдельных лиц, размещающих и распространяющих на сайтах информационной сети экстремистские материалы, а также комплекс мер по их блокированию. Необходимы более эффективные меры органов государственной власти и местного самоуправления, во взаимодействии с общественными организациями, в профилактике проявлений экстремизма в религиозной и молодежной среде. В этой связи, положительной видится идея создания в РСО-Алания Центра профилактики экстремизма.[111]

Повышению эффективности проводимой политики в сфере противодействия экстремизму, в том числе и в сети Интернет, будет способствовать разработка общегосударственной комплексной программы, охватывающей не только правоохранительный, но и политический, социальный, экономический, идеологический, пропагандистский, информационный и другие аспекты.

Однако важно учитывать, что только силами государства противостоять этому деструктивному явлению современности прак-

[110] Сигарев А.В. Правовое регулирование противодействия экстремизму / А.В. Сигарев. Новосибирск: Изд-во СибАГС, 2015. С. 119.

[111] Центр профилактики экстремизма создадут в Северной Осетии. / [Электронный ресурс] // Режим доступа: http://sevosetia.ru/Article/Index/332598

тически невозможно, а потому необходима поддержка со стороны граждан и институтов гражданского общества.[112]

В качестве еще одной проблемы можно выделить недостаточное финансирование мероприятий по противодействию терроризму и экстремизму в рамках государственных и муниципальных программ.

На сегодняшний день одной из важных проблем выступает недостаточное нормативно-правовое регулирование в рамках международного взаимодействия государств в сфере противодействия экстремизму и терроризму в информационно-коммуникационном пространстве.

Так, в настоящее время отсутствует международный нормативно-правовой акт, регламентирующий взаимодействие государств в сфере противодействия экстремизму и терроризму в информационно-коммуникационном пространстве. Проблема осложняется использованием государствами различных, как правило, отличных друг от друга подходов к нормативно-правовому регулированию антиэкстремистской деятельности. Что, конечно, не способствует эффективному сотрудничеству в борьбе с экстремизмом в сети Интернет.

По нашему мнению, было бы целесообразным принятие соответствующих документов международного уровня, которые бы закрепили как правовой статус международного информационного пространства, так и механизмы урегулирования споров, и вопросы оказания правовой помощи.

Важно отметить опыт сотрудничества в сфере противодействия экстремистским проявлениям в рамках Шанхайской организации сотрудничества. Так, Федеральным законом от 26 июля 2019 года №196-ФЗ была ратифицирована Конвенция Шанхайской организации сотрудничества по противодействию экстремизму.

В соответствии со ст. 7 Конвенции, стороны разрабатывают и осуществляют меры на национальном уровне по противодей-

[112] Золоева З.Т., Койбаев Б.Г. Некоторые проблемы правового противодействия экстремистским проявлениям в информационно-телекоммуникационной сети Интернет // Гуманитарные и юридические исследования. 2018. №4. С. 170-175.

ствию экстремизму, которые могут включать, в том числе, меры по:

- усилению пропагандистской деятельности в сфере противодействия экстремизму и контрпропагандистскую работу против распространения экстремистской идеологии, в том числе в средствах массовой информации (СМИ) и сети «Интернет»;

- мониторингу СМИ и сети «Интернет» в целях своевременного выявления и пресечения распространения экстремистской идеологии;

- ограничению доступа к экстремистским материалам, размещенным в информационно-телекоммуникационных сетях.[113]

Несомненно, принятие Конвенции позволит повысить эффективность борьбы с распространением экстремизма в сети Интернет. Однако Конвенция еще не принята, кроме того, она носит региональный характер. По нашему мнению, существует необходимость разработки универсального международного документа, который бы регулировал борьбу с экстремизмом в сети «Интернет».

[113] Конвенция Шанхайской организации сотрудничества по противодействию экстремизму. Ратифицирована Федеральным Собранием (Федеральный закон от 26 июля 2019 года №196-ФЗ // Собрание законодательства Российской Федерации. 2019. №30. Ст. 4098). Конвенция вступила в силу для Российской Федерации 12 октября 2019 года // Собрание законодательства Российской Федерации. 2019. №47. Ст. 6560.

ЗАКЛЮЧЕНИЕ

Политика цифровизации не системна, не объединена общим ценностно-смысловым началом. Противоречивость политики цифровизации в современном обществе определяется попыткой совместить прогрессивные задачи и неэффективные бюрократические средства их разрешения. Характер развернувшейся цифровизации ставит вопрос о масштабных преобразованиях в деятельности всей общественно-политической и социально-экономической системы, объединенных общей ценностно-смысловой основой. В осмыслении характера направлений цифровизации общества повышается уровень востребованности научного анализа. Появление новых технических возможностей не определяет готовность субъектов политико-правового процесса ими рационально распоряжаться.

Раскрытие рисков цифровизации – задача, прежде всего, политико-правового знания. Активизировав весь свой накопленный веками потенциал, оно способно противопоставить поверхностному, прагматичному знанию глубинные смыслы национальной безопасности и всего человеческого существования. Поставив «цифру» под контроль современных наук, включив цифровые практики в контекст культуры в широком смысле, человек продлит свое существование в качестве существа разумного и ответственного за этот мир.

Отметим при этом, что речь не идет об отрицании положительной роли техники в общественном развитии. Это, несомненно, достижение культуры, которое и дальше в своем развитии способно обеспечить современный прогресс. Но чтобы человек и техника «шли в одном направлении», необходимо обретение ими целенаправленной связи, основанной на понимании сущностей одного и другого.

В XXI веке термины «информационное общество», «информатизация» и «цифровизация» прочно заняли свое место в лексиконе специалистов в области информации, политических деяте-

лей, экономистов, преподавателей и ученых. Под цифровизацией понимается особый социально-исторический процесс, который выражается через содержание информационной революции и ведет к новому состоянию общества.

Ряд ученых рассматривают информатизацию и цифровизацию как системно-деятельностный процесс овладения информацией как ресурсом управления и развития с помощью средств информатики с целью создания информационного общества, и на этой основе – дальнейшего продолжения прогресса цивилизации.

Воплощением процесса информатизации в современном обществе стал Интернет. В этой связи можно согласиться с мнением, что информационное общество разные государства строят именно на базе интернет-технологий. Интернет сейчас больше, чем некая информационная технология. Он является не только высокоэффективным инструментом решения наших стратегических и повседневных задач.

Необходимо принимать во внимание тот факт, что почти во всех сферах жизнедеятельности человека информация становится определяющим ресурсом. Стержневым фундаментом новой информационной эры является сеть Интернет, объединяющая как отдельных людей и их субкультуры, так и целые народы между собой, а также бизнес-среду всех уровней.

Становится очевидным, что интернет-среда становится не только воплощением стремительно происходящих технико-технологических изменений в социуме, но своего рода индикатором успешности происходящих процессов. Создаваемая посредством глобальной компьютерной сети информационно-коммуникационная среда общественной жизни становится системным инструментом воплощения различных новшеств в сфере приема-передачи сообщений.

Нужно обратить внимание на то, что в современном обществе возникают новые угрозы человечеству, что общество в значительной степени оказывается неподготовленным к этим угрозам. К примеру, массовое хакерство, т.е. вероломное проникновение в информационные системы, перешло на качественно новый уровень и приобрело характер информационного терроризма. А вторжение в информационные системы атомных электростан-

ций, проникновение в базы данных военных, финансовых, хозяйственных, коммерческих структур и т.д. может повлечь за собой непоправимые последствия. Нередко оказывается так, что менее информатизированная и компьютеризированная сторона общественной жизни оказывается более защищенной от информационных террористов, способной устоять перед этими угрозами.

В условиях социума начала XXI в. возникают условия для массового копирования и распространения вредной, антисоциальной информации. В этой связи стоит согласиться с мнением о том, что информационно-телекоммуникационные сети общего пользования (в частности, Интернет) являются наиболее перспективными средствами пропаганды экстремистских материалов ввиду оперативности предоставляемых сведений, относительной дешевизны технологии создания и распространения информации, сложности, а в большинстве случаев невозможности привлечения к ответственности лиц, размещающих такие материалы, в силу отсутствия системы международных соглашений и законодательства, регулирующих вопросы борьбы с распространением экстремистских материалов на сайтах зарубежных государств.

Растущая эффективность информационных и телекоммуникационных средств воздействия на аудиторию создает социально опасную ситуацию, заключающуюся в создании условий для отрицательного воздействия на сознание и поведение людей с использованием современных аудиовизуальных средств и технологий. Как справедливо отмечают в этой связи исследователи, нынешний этап развития информационных отношений характеризуется возможностью информационного воздействия на индивидуальное и общественное сознание, вплоть до угрозы информационных войн, в результате чего неизбежным противовесом свободы информации становится проблема информационной безопасности.

Особую опасность для общества таят в себе информационные войны и пропагандистские кампании, сопровождающие межгрупповые, межнациональные, межгосударственные конфликты. Наибольшую обеспокоенность у исследователей вызывает информационное сопровождение открытых военных конфликтов. В современных военных конфликтах активное применение нахо-

дят разнообразные технологии влияния на массовое сознание. То, что в мирном противоборстве компаний называется реклама и продвижение, в военных конфликтах является пропагандой и информационно-психологическим воздействием на противника. Технологии пропаганды и информационно-психологического воздействия постоянно усовершенствуются и развиваются с внедрением в нашу жизнь более технологичных устройств коммуникации и информирования.

Основная опасность отмеченных коммуникативных действий заключается в непредсказуемом, неконтролируемом характере их последствий. Коммуникатор, спровоцировав подобную «электризацию» информационно-коммуникационной (а шире – политической, экономической, социальной, культурной) среды, не может в полной мере контролировать и прогнозировать последствия своих действий. Одним из негативных социальных последствий подобной безответственной деятельности выступает модификация традиционного облика экстремизма, появление такой его разновидности, как информационный экстремизм.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Национальные (федеральные) источники, нормативные и правовые акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. 25 декабря.

2. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2013-2018 годы от 26 апреля 2013 года №П.1069.

3. Федеральный закон РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.03.2019 г.).

4. Федеральный закон «О противодействии экстремистской деятельности» от 25 июля 2002 г. №114-ФЗ (в редакции Федеральных законов Российской Федерации от 24 июля 2007 г. №211-ФЗ; от 29 апреля 2008 г. №54-ФЗ) // Российская газета. 2002. 30 июля.

5. Федеральный закон от 17.06.1996 №74-ФЗ «О национально-культурной автономии» (В ред. Федер. закона от 30.11.2005 №146-ФЗ) // Российская газета. 1996. 25 июня.

6. Федеральный закон «О гарантиях прав коренных малочисленных народов Российской Федерации» от 30.04.1999 №82-ФЗ (В ред. Федер. закона от 22.08.2004 №122-ФЗ) // Российская газета. 1999. 12 мая.

7. Федеральный закон «О свободе совести и о религиозных объединениях» от 26.09.1997 №125-ФЗ (В ред. Федер. закона от 28.02.2008 №14-ФЗ) // Российская газета. 2008. 5 марта.

8. Федеральный Закон «О противодействии терроризму» от 6 марта 2006 г. №35-ФЗ (В ред. Федер. закона от 27 июля 2006 года №153-ФЗ). 4-е изд. М.: Ось-89, 2008. 48 с.

9. Федеральный закон «О некоммерческих организациях» от 12.01.1996 №7-ФЗ (В ред. Федер. закона от 02.02.2006 №19-ФЗ) // Российская газета. 1996. 24 января.

10. Федеральный закон от 19.02.1993 №4528-1 «О беженцах» (В ред. Федер. закона от 18.07.2006 №121-ФЗ) // Российская газета. 1997. 3 июня.

11. Федеральный закон «Об общественных объединениях» от 19.05.1995 №82-ФЗ. (В ред. Федер. закона от 02.02.2006 №19-ФЗ) // Российская газета. 1995. 25 мая.

12. Концепция государственной национальной политики Российской Федерации // СЗ РФ. 1996. №25. Ст. 3010.

13. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. №203.

14. Указ Президента РФ «Об утверждении Концепции государственной национальной политики Российской Федерации от 15 июня 1996 года №909 // СЗ РФ. 1996. №25. Ст. 3010.

15. Указ Президента РФ от 15 февраля 2006 г. №116 «О мерах по противодействию терроризму» (В ред. Указа Президента №1188 от 08.08.08) // Российская газета. 2006. 17 февраля.

16. Указ Президента РФ от 27 октября 1997 г. №1143 «О комиссии при Президенте Российской Федерации по противодействию политическому экстремизму в Российской Федерации» // Российская газета. 1997. 30 октября.

Республиканские нормативно-правовые акты

17. Конституция Республики Северная Осетия – Алания. Принята Верховным Советом Республики Северная Осетия 12 ноября 1994 г. (В редакции Конституционного закона РСО-Алания от 19.07.2000 г. №10-РВ). Владикавказ: Изд-во ОАО «ИПП им. Гассиева», 2006. 80 с.

18. Закон Республики Северная Осетия – Алания от 28.05.2008 №21-РЗ «О внесении изменений в Закон Республики Северная Осетия – Алания «О миссионерской деятельности на территории Республики Северная Осетия – Алания» // Северная Осетия. 2008.

19. Закон Республики Северная Осетия – Алания от 10.12.2007 №66-РЗ «О Республиканской целевой программе по противодействию экстремистским проявлениям в Республике Северная Осетия – Алания на 2008-2010 годы // Северная Осетия. 2008. 16 января.

20. Государственная программа Республики Северная Осетия – Алания «Развитие межнациональных отношений в Республике

Северная Осетия – Алания на 2014-2018 годы», от 15 ноября 2013 г. №416.

21. Указ Главы Республики Северная Осетия – Алания №90 от 04.05.2007 г. «О мерах по противодействию терроризму на территории Республики Северная Осетия – Алания».

22. Постановление Правительства РСО-Алания от 03.08.2007 г. №188 «Программа развития и гармонизации межнациональных отношений в РСО-Алания».

23. Устав Международного общественного движения «Высший Совет Осетин». Владикавказ, 2011.

Исследования, монографии, сборники

24. Абдулатипов Р.Г. Национальная политика от концепции к реализации. М.: Славянский диалог, 1997. 111 с.

25. Абдулатипов Р.Г. Управление этнополитическими процессами. Вопросы теории и практики. М.: Славянский диалог, 2001. 340 с.

26. Абдулатипов Р.Г. О федеративной и национальной политике Российского государства. М.: Славянский диалог, 1995. 63 с.

27. Абдулатипов Р.Г. Авторитет разума. М.: Славянский диалог, 1999. 319 с.

28. Абдулатипов Р.Г. Национальный вопрос и государственное устройство России. М.: Славянский диалог, 2000. 656 с.

29. Абдулатипов Р.Г. Сущность нации, этноса: ответ сторонникам безнациональности. М.: Славянский диалог, 1999. 32 с.

30. Абдулатипов Р.Г. Обустройство народов: российская модель. М.: Славянский диалог, 1999. 32 с.

31. Абдулатипов Р.Г. Историческая многонациональность в России: политика, мораль, управление. М.: Славянский диалог, 1999. 62 с.

32. Абдулатипов Р.Г. О Федеративной и национальной политике Российской Федерации на современном этапе // Этнопанорама. 2001. №3. С. 6.

33. Абдулатипов Р.Г. Предмет и перспективы национальной политики // Этнопанорама. 1999. №1. С. 2.

34. Абазалиева М.М. Особенности современных националь-

ных процессов на Северном Кавказе: Автореф. дисс… канд. полит. наук. Черкесск, 2006. 27 с.

35. Авксентьев А.В. Этнические проблемы: современность и культура межнационального общения. Ставрополь, 1993. 222 с.

36. Актуальные проблемы теории и практики федеративных и национальных отношений. М.: Луч, 1993. 22 с.

37. Артановский С.Н. Межнациональное государство с точки зрения культурологии // Философские науки. 1990. №8.

38. Арутюнян Ю.В. Общее и национально-особенное в социально-культурном облике сельского населения СССР // История СССР. №6.1985.

39. Амелин В.В. Вызовы мобилизованной этничности: конфликты в истории советской и постсоветской государственности. М., 1997. 318 с.

40. Амелин В.В. Проблемы равного доступа к власти национальных групп в полиэтнических регионах России // Этнопанорама. 2000. №2. С. 13-20.

41. Антименко О.О. Экстремизм и СМИ: спасет ли нас общественный контроль? // Экстремизм и средства массовой информации: Мат-лы Всерос. науч.-практ. конф. / Под ред. В.Е. Семенова. СПб., 2006. С. 151.

42. Аствацатурова М.А. Северный Кавказ: перспективы и риски (Трансформация регионального этнополитического пространства). М., 2011. 192 с.

43. Асташова А.Н., Кирюшин А.Н. Психологическая война как война будущего // Экстремизм, конфликты и войны: история и современность: Труды Междунар. конф. Воронеж, 2010. С. 188.

44. Бабаков В.Г. Национальное сознание и национальная культура. М., 1996. 70 с.

45. Багаева А.А. Проблемы противодействия экстремизму и терроризму: историко-правовой аспект // Актуальные проблемы противодействия экстремизму. Материалы Международной научно-практической конференции. Северо-Кавказский горно-металлургический институт (государственный технологический университет). 2018. С. 275-286.

46. Багаева А.А. Проблемы государственной политики по противодействию экстремизму и терроризму в СМИ и Интер-

нет-пространстве // Право и государство, общество и личность: история, теория, практика. Сборник научных статей участников VII Всероссийской научно-практической конференции с международным участием. 2018. С. 30-36.

47. Бааль Н.Б. Молодежные экстремистские организации в постсоветской России // История государства и права. 2007. №11. С. 26.

48. Баликоев Т.М., Койбаев Б.Г., Баликоев А.Т. Межнациональные отношения в Северной Осетии: механизмы регулирования. Владикавказ, 2015. 103 с.

49. Баранов А.В. Взаимодействие акторов региональных политических процессов в постсоветской России. М.: Социально-политическая мысль, 2007. 192 с.

50. Баранов А.В. Политические институты федерализма как фактор этнической конфликтности (на материалах Косово и Чечни) // Федерализм и российские регионы: Сб. статей. М.: ИНИОН РАН, 2006. С. 78-94.

51. Баранов А.В. Урегулирование этнополитических конфликтов как задача национальной политики России в Южном федеральном округе // Конфликты и сотрудничество на Северном Кавказе: управление, экономика, общество: Сборник тезисов выступлений на Международной научно-практической конфе¬ренции 29-30 сентября 2006 г., Ростов-на-Дону – Горячий Ключ: Изд-во Северо-Кавказской академии гос. службы, 2006. С. 87-89.

52. Баранов А.В., Вартумян А.А. Политическая регионалистика. Курс лекций. Вып. 3. М.: Изд-во РГСУ «Союз», 2004.

53. Баранов В.В., Исаев Е.А. О правовом регулировании деятельности органов внутренних дел по противодействию экстремистским проявлениям в информационном пространстве // 2020. №2 (54). С. 14-20.

54. Барбашин М.Ю. Мифология «Исторической справедливости» в этнополитических конфликтах как фактор легитимации этнических элит // Политическая мифология и историческая наука на Северном Кавказе / Отв. ред. В.В. Черноус. Ростов-на-Дону, 2004.

55. Барт Ф., Пильщиков И.А. Этнические группы и социальные границы. М.: Новое издательство, 2006. 200 с.

56. Бахлова И.В. Региональные политические элиты в федеративном государстве // Политология. Саранск: Изд-во Мордов. ун-та, 2000.

57. Башкатов Л.Н., Беляев А.Е., Игнатьев А.А., Изоитко С.И., Устинков А.В. Основные проблемы уголовно-правовой оценки проявлений экстремизма и терроризма // Право и безопасность. №3-4. 2007.

58. Беляев Д.А. Интернет как основа информационного общества / [Электронный ресурс] // Режим доступа: http://www.gosbook.ru/system/files/documents/2011/09/01/k-1-1-11-informatizacija.pdf.

59. Березкина О.П. ТВ-технологии как средство формирования культуры насилия и управления массовым сознанием // Экстремизм и СМИ... СПб., 2006. С. 91.

60. Белова Т.П., Щепеткова Е.В. Информационный фактор терроризма в оценках студентов г. Москвы и г. Иванова // Экстремизм и СМИ... СПб., 2006. С. 87.

61. Березин Г.В. Особенности влияния СМИ на формирование современных политических ориентаций россиян (на примере телевидения): Автореф. дисс... канд. филос. наук. М., 2000.

62. Бирюков С.В. Региональная политическая власть: от концептов к интегративной модели // Вестник МГУ. Сер. 18. Социология и политология. 2003. №1.

63. Бирюков В.В. Еще раз об экстремизме // Адвокат. 2006. №12.

64. Боришполец К.П. Постсоветское пространство в этнополитическом измерении // Вест. Моск. ун-та. 1998. Сер. 18. №3. С. 30.

65. Боров А.Х. Проблемы формирования современной политической элиты в Северо-Кавказском регионе // Элиты и будущее России: взгляд из регионов: Сб. материалов Международной научно-практической конференции / Отв. ред. В.Г. Игнатов. Ростов-на-Дону: СКАГС, 2007.

66. Бугай Н.Ф., Гонов А.М. Северный Кавказ: новые ориентиры национальной политики (90-е годы XX века). М., 2004. 368 с.

67. Вартумян А.А. Национализм как средство коллективной мобилизации и психологической компенсации в региональных конфликтах // Материалы Международного «круглого стола» экс-

пертов «Региональные конфликты в полиэтничном регионе: методы анализа, прогнозирования и конструктивной деэскалации», Институт социологии РАН, СГУ (2 октября 2006 г.). Ставрополь, 2006.

68. Вартумян А.А. Региональная политика в Российской Федерации // Ученые записки. 2004. №2. С. 124-129.

69. Вартумян А.А. Региональный политический процесс: динамика, особенности, проблемы. М.: РГСУ, 2004. 179 с.

70. Вартумян А.А. Юг России: процесс регионального социально-политического развития // Россия: Центр и регионы. М.: ИСПИ РАН, 2002.

71. Вебер М. Избранные произведения. М.: Прогресс, 1990. 804 с.

72. Властные элиты современной России в процессе политической трансформации / Отв. ред. В.Г. Игнатов, О.В. Гаман-Голутвина, А.В. Понеделков, А.М. Старостин. Ростов-на-Дону: СКАГС, 2004. 295 с.

73. Бидихов С.А. Пути нормализации межэтнической напряженности на Северном Кавказе. Стабилизация межэтнических и социально-культурных отношений на Кавказе. Этнодиалоги. М.: Этносфера, 1999.

74. Вдовин А.И. Особенности этнополитических отношений и формирование новой государственности в России. М., 1993. 72 с.

75. Вердиев Р.Т. Особенности современной Осетии. М., 2009. 182 с.

76. Власть и общество в постсоветской России: новые практики и институты. М., 1999. 224 с.

77. Галкина Е.В. Противодействие политическому экстремизму и терроризму: новый взгляд // Теория и практика общественного развития. Краснодар: Издат. дом «Хорс», 2014. №1. С. 341-344.

78. Галяшина Е.И., Никишин В.Д. Особенности административных дел о признании информационных материалов экстремистскими и их экспертиза в аспекте безопасности интернет-коммуникации // Актуальные проблемы российского права. 2021. Т. 16. №7. С. 159-167.

79. Гатеев В.М. Межнациональные и этнополитические процессы на Северном Кавказе в период демократических реформ (1991-2005 гг.). Владикавказ, 2005. 168 с.

80. Гацоева Н. Угрозы в сети и наяву // Северная Осетия. 23.03.2021.

81. Геллнер Э. Нации и национализм. М.: Прогресс, 1991. 320 с.

82. Государственная служба РФ и межнациональные отношения / Тавадов Г.Т. и др.; ред. кол.: Абдулатипов Р.Г. и др. М.: Луч, 1995. 265 с.

83. Грачев С.И., Герасин О.Н., Колобов А.О., Ливерко М.И. Проблемные аспекты в информационной политике и информационной безопасности России // Вестник Нижегородского университета им. Н.И. Лобачевского. №1. 2012. С. 290.

84. Гнатюк О.Л. Алармизм как негативная асимметрия, или Новая функция российских СМИ? // Экстремизм и СМИ... СПб., 2006. С. 17.

85. Григорьев С.И. Актуальные проблемы анализа жизненных сил национальных общностей в России // Вестник МГУ. Сер. 18. 2000. №2. С. 95.

86. Губогло М.Н. Национально-культурные автономии и объединения. Антология в 3 т. М.: ЦИМО РАН, 1995.

87. Губогло М.Н. Религиозность, этничность, государственность // Этнопанорама. 2000. №3. С. 2-11.

88. Губогло М.Н. Ассамблея народов России (концептуальные размышления) // Этнопанорама. 1999. №1. С. 6-13.

89. Гундарь О.Н., Галкина Е.В., Гундарь Е.С. Политический экстремизм в современном мире. Безопасность и противодействие терроризму. Учебное пособие. Ставрополь: Изд-во СГУ, 2009. 139 с.

90. Дзахова Л.Х., Чихтисов Р.А. Межэтнические отношения и религиозная ситуация в Республике Северная Осетия – Алания в первом квартале 2015 года // Состояние межнациональных отношений и религиозная ситуация в СКФО (по состоянию на первое полугодие 2015 г.): экспертный доклад / Под ред. В.А. Тишкова. Ставрополь: Изд-во СКФУ, 2015. С. 96.

91. Дзеранов Т.Е., Койбаев Б.Г. Мониторинг государствен-

но-конфессиональных отношений в Республике Северная Осетия – Алания и отношения населения к экстремистским проявлениям: Отчет по итогам исследовательской работы. Владикавказ, 2012. С. 69-70.

92. Дзидзоев В.Д. К вопросу об исторической подоплеке некоторых межнациональных проблем и конфликтов // Проблемы формирования исторического сознания. Ростов-на-Дону, 1995. С. 51-59.

93. Дзидзоев В.Д. Национальная политика: уроки опыта. Владикавказ, 2002. 245 с.

94. Дзидзоев В.Д. Кавказ конца XX века: тенденции этнополитического развития (историко-политологическое исследование). Владикавказ, 2004. 358 с.

95. Дзидзоев В.Д. Осетия в эпоху больших потрясений и перемен (исторический и политико-правовой анализ постсоветской истории). Владикавказ, 2010. 128 с.

96. Дзидзоев В.Д. От искажений отдельных исторических фактов до фальсификации осетино-ингушских отношений (исследование конкретного политико-правового казуса). Владикавказ, 2010. 278 с.

97. Дзидзоев В.Д., Никаев Р.М. Современные этнополитические процессы на Северном Кавказе как вызовы и угрозы национальной безопасности Российской Федерации. Владикавказ, 2014.

98. Джанаев Х.Г. Социально-политические основы становления и развития Республики Алания в системе трансформационных координат XXI века: Автореф. дисс… докт. полит. наук. РАН ИСПИ. М., 2006.

99. Джунусов М.С. О мере своеобразия национальных культур // Социологические исследования. 2002. №5. С. 125-128.

100. Дигуров А.Б. Ценностные ориентации как фактор политического поведения граждан России в постсоветский период. (На примере Республики Северная Осетия – Алания): Автореф. дисс… канд. полит. наук. М., 2004. 27 с.

101. Дробижева Л.М. Социальные проблемы межнациональных отношений в постсоветской России. М.: Центр общечеловеческих ценностей, 2003. 376 с.

102. Дробижева Л.М. Демократизация и образы национализма в РФ 90-х годов. М., 1996. 243 с.

103. Дробижева Л.М. Этничность в современной России: этнополитика и социальная практика // Этнопанорама. 2002. №1. С. 1-9.

104. Дороченко А.И. Межнациональные отношения и национальная политика в России: актуальные проблемы теории, истории и современной практики. СПб., 1995. 199 с.

105. Жалинский А.Э. Условия эффективности профилактики преступлений. М., 1978. С. 47.

106. Золоев С.Т., Багаева А.А. Основы реализации государственной политики по противодействию экстремизму и терроризму в современных СМИ и интернет-пространстве // Развитие интеллектуально-творческого потенциала молодежи: из прошлого в современность. Материалы I Международной научно-практической конференции / Под общ. ред. проф. С.В. Беспаловой. 2018. С. 275.

107. Золоева З.Т. Некоторые проблемы реализации права на доступ к информации (на материалах РСО-Алания) (Часть 1) // Информационные ресурсы России. 2017. №1 (155). С. 40-45.

108. Золоева З.Т. Некоторые проблемы реализации права на доступ к информации (на материалах РСО-Алания) (Часть 2) // Информационные ресурсы России. 2017. №2 (156). С. 20-23.

109. Золоева З.Т. Правовые аспекты государственной политики в сфере информатизации регионов // Вестник Северо-Осетинского государственного университета имени К.Л. Хетагурова. 2014. №1. С. 140-144.

110. Золоева З.Т. Правовые аспекты противодействия экстремизму в условиях информационного общества // Труды СКГМИ (ГТУ). 2017. №24. С. 142-146.

111. Золоева З.Т. Информационный экстремизм в условиях глобализации и информатизации социума // Актуальные проблемы противодействия экстремизму. Материалы Международной научно-практической конференции. Северо-Кавказский горно-металлургический институт (государственный технологический университет). 2018. С. 293-297.

112. Золоева З.Т. Проблемы борьбы с экстремистскими проявлениями в сети Интернет на территории РСО-Алания // Актуаль-

ные проблемы юридической науки и практики. Материалы Международной научно-практической конференции. 2018. С. 301-305.

113. Золоева З.Т., Койбаев Б.Г. Некоторые проблемы правового противодействия экстремистским проявлениям в информационно-телекоммуникационной сети Интернет // Гуманитарные и юридические исследования. 2018. №4. С. 170-175.

114. Золоева З.Т. Противодействие экстремистским проявлениям в условиях развития информационного общества: правовые аспекты // VII Международный молодежный юридический форум «Экстремизму – отпор». Сборник научных статей материалов Международной научно-практической конференции / Под ред. Кокоевой Л.Т., Цалиева А.М., 2019. С. 234-243.

115. Золоева З.Т., Гуриева Э.Г. Роль средств массовой информации в противодействии экстремизму // Труды СКГМИ (ГТУ). 2019. №26. С. 92-97.

116. Золоева З.Т., Койбаев Б.Г. Из истории государственной политики РСО-Алания в сфере формирования информационного общества в 1995-2010 гг. // Вестник Северо-Осетинского государственного университета имени К.Л. Хетагурова. 2018. №2. С. 35-38.

117. Зорькин В.Д. Право в цифровом мире: Размышление на полях Петербургского международного юридического форума // Российская газета. Столичный выпуск. №115.

118. Зорин В.Ю. Национальный вопрос в государственных Думах России. М.: Информационно-издательское агентство «Русский мир», 1999. 520 с.

119. Исследование динамики развития религиозной ситуации и форм противодействия экстремистской идеологии в Правобережном и Кировском районах РСО-Алания: Аналитический отчет. Владикавказ, 2016. С. 6-7. 298 с.

120. Калинина К.В. Национальные меньшинства в России. М.: Луч, 1993. 86 с.

121. Канукова З.В. Старый Владикавказ: Историко-этнологическое исследование. Владикавказ, 2002. 146 с.

122. Канукова З.В. Диаспоры в Осетии: исторический опыт жизнеустройства и современное состояние. Владикавказ, 2009. 172 с.

123. Карсанова Е.С., Койбаев Б.Г., Исмаилов М.А. Рецензия на монографию В.Д. Дзидзоева и Р.М. Никаева «Современные этнополитические процессы на Северном Кавказе как вызовы и угрозы национальной безопасности Российской Федерации» // Вестник Владикавказского научного центра. 2014. Т. 14. №1. С. 77.

124. Карягина А.В. Информационный экстремизм в современном государственно-правовом пространстве // Философия права. 2010. №4. С. 105-107.

125. Кирюшин А.Н., Асташова А.Н. Информационная война: сущность и содержание // Экстремизм, конфликты и войны: история и современность: Труды Междунар. конф. Воронеж, 2010. С. 196.

126. Козлов А.А., Козлов Н.А. СМИ, экстремизм, молодежь // Экстремизм и СМИ... СПб., 2006. С. 17-18.

127. Козлов В.И. Этнос. Нация. Национализм: сущность и проблематика. М.: Старый сад, 1999. 343 с.

128. Козер Л. Функции социального конфликта. М.: Идея-пресс: Дом интеллектуальной книги, 2000. 205 с.

129. Койбаев Б.Г. Проблемы взаимоотношения региональной элиты и населения в общественно-политической жизни // Гражданское общество. Владикавказ, 2006. №1.

130. Койбаев Б.Г. Теракт в Беслане: глобальные и региональные аспекты, политические последствия // Кавказ в системе международных отношений. Университет Александра Дубчека в Тренчине. Тренчин, 2006. С. 175-182.

131. Койбаев Б.Г., Курбанов Р.Н. Противодействие экстремистской деятельности в Республике Северная Осетия – Алания: политико-правовые аспекты. Владикавказ: ИПП им. Гассиева, 2010. 240 с.

132. Койбаев Б.Г., Бязров А.В. Современный экстремизм: сущность, содержание и формы проявления: международный и региональный аспекты. Владикавказ, 2012. 154 с.

133. Койбаев Б.Г., Баликоев Т.М. Национально-культурная автономия (НКА) как механизм реализации национальной политики // Вестник Северо-Осетинского государственного университета им. К.Л. Хетагурова. 2014. №3. С. 64.

134. Койбаев Б.Г. Гармонизация межнациональных отношений в Республике Северная Осетия как фактор противодействия экстремизму и терроризму. Владикавказ: ИПЦ ИП Цопанова А.Ю., 2016. 302 с.;

135. Койбаев Б.Г., Багаева А.А., Золоева З.Т. Актуальные проблемы в сфере противодействия экстремистским и террористическим проявлениям в Республике Северная Осетия – Алания: монография / Б.Г. Койбаев, А.А. Багаева, З.Т. Золоева; СКГМИ (ГТУ). Владикавказ: ИПЦ ИП Цопанова А.Ю., 2019. 290 с.

136. Койбаев Б.Г., Золоева З.Т. Некоторые аспекты административно-правового регулирования деятельности органов исполнительной власти в условиях цифровой реальности // Гуманитарные и юридические исследования. 2020. №1. С. 119-124.

137. Койбаев Б.Г., Золоева З.Т. Правовые основы формирования и развития информационного общества в регионе (на примере Республики Северная Осетия – Алания) // Гуманитарные и юридические исследования. 2017. №2. С. 138-143.

138. Кокоева Л.Т., Чеджемов С.Р. К проблеме моральной и материальной компенсации пострадавшим в результате экстремистских деяний // Экстремизму – отпор! Сборник статей по материалам IX Международного молодежного форума / Под ред. Г.В. Синцова, Л.Т. Кокоевой. Пенза, 2020. С. 13-18.

139. Конфликты в современной России (проблемы анализа и урегулирования) / Под ред. Е.И. Степанова. М.: Эдиториал УРСС, 1999. 344 с.

140. Константинова Н.П. Экстремизм и СМИ: отражение в массовом сознании молодежи // Экстремизм и СМИ... СПб., 2006. С. 171.

141. Крыштановская О.В. Политические реформы Путина и элита // Экономика и общество. 2003. №4.

142. Концепция государственной национальной политики РФ: опыт, реализация (2002). М., 2003.

143. Кудрин В.С. Молодежный экстремизм: причины возникновения, технологии предупреждения. Учебное пособие / В.С. Кудрин, А.И. Юдина. Кемерово: Кемеровский государственный институт культуры, 2016. 160 с. ISBN 978-5-8154-0326-0. – Текст:

электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/55796.html

144. Кузнецов И.И. Геополитическое самоутверждение региона// Полис. 2000. №3. С. 117-127.

145. Кулаковский А.В., Соловьев В.А. Северная Осетия и Ингушетия: Опыт постконфликтного строительства новых взаимоотношений. Владикавказ, 2003. 134 с.

146. Куракина Т.Н. Управление культурными процессами в регионе: опыт, тенденции. М.: Луч, 1994. 146 с.

147. Кутахов Ю.Л., Явчуновская Р.А. Человек. Полиэтничный мир. Безопасность. СПб.: Изд-во Разумовой Н.А., 1998. С. 404.

148. Ланцев И.А. Глобализм и проблемы информационно-психологической безопасности // Экстремизм и СМИ... СПб., 2006. С. 46.

149. Марченко М.Н. Глобализация и ее воздействие на современное национальное государство (методологический аспект) // Теоретико-методологические проблемы права. М., 2007. С. 65.

150. Магометов А.А. Межнациональные отношения, интернациональное и патриотическое воспитание: этнопсихологический аспект. М., 2004. 368 с.

151. Мамсуров Т.Д. Этнополитические и региональные проблемы развития российского федерализма (на примере Республики Северная Осетия-Алания): Автореф. дисс…докт. полит. наук / РАН. ИСПИ. М., 2002.

152. Медведев Н.П. Институт консенсуса и проблемы федерализма в России // Конституционно-правовые проблемы развития Российского федерализма. М., 2000.

153. Мельник Г.С. Особенности освещения в СМИ проблемы иномерности // Экстремизм и СМИ... СПб., 2006. С. 48.

154. Михайлов В.А. Национальная политика России как фактор государственного строительства. М., 1995. 46 с.

155. Мозговой В.Э. Информационный экстремизм в условиях глобализации и информатизации социума // Общество и право. 2015. №1 (51). С. 309-313. С. 309.

156. Мозговой В.Э. Информационный экстремизм в условиях социо-коммуникативных трансформаций российского общества // Дисс. к. с. н. Краснодар, 2015. С. 3.

157. Морозов И.Л. Политический экстремизм: особенности эволюции при переходе от индустриального общества к информационному: Монография. Волгоград, 2007. С. 36.

158. Морозов И.Л. Политический экстремизм: Учеб. пособие. Волжский, 2008. С. 39.

159. Науменко Т.В. Социология массовой коммуникации. СПб., 2005. С. 56.

160. На территории Северной Осетии заблокировано более 90 экстремистских Интернет-ресурсов. / [Электронный ресурс] // Режим доступа: http://gradus.pro/145331-2/

161. Национальная доктрина России: проблемы и приоритеты. М.: Обозреватель, 1994. 501 с.

162. Национальная политика в РФ: материалы Международной научно-практической конференции. М.: Наука, 1993. 184 с.

163. Национальная политика России: история и современность. М.: Информационно-издательское агентство «Русский мир», 1997. 680 с.

164. Национально-культурная автономия: проблемы и суждения. М.: Этнодиалоги, 1998. 168 с.

165. Некрасова Е.В. Информационный аспект экстремизма и терроризма и деструктивные тенденции в СМИ // Вестник Российского университета дружбы народов. Серия: Социология. 2013. №6. С. 57-65.

166. Никитин В.И. Национальный вопрос: национальная политика России в начале XXI века // Этнопанорама. 2001. №2. С. 2.

167. Основы национальных и федеративных отношений: Учебник / Под общ. ред. Р.Г. Абдулатипова. М.: Изд-во РАГС, 2001. 352 с.

168. О проекте Федерального закона «Об основах государственной национальной политики». М., 2002. 112 с.

169. О роли Ассамблеи народов России и ее региональных отделений в реализации концепции государственной национальной политики РФ на современном этапе. М., 2002.

170. Основы теории коммуникации / Под ред. М.А. Василика. М., 2003. С. 443.

171. Павлова Е.Д. Информационный терроризм со стороны

СМИ: целенаправленное формирование культа насилия // Экстремизм и СМИ... СПб.: Астерион, 2006. С. 126-127.

172. Панферова В.В. Информационная политика в современной России // Социально-гуманитарные знания. №5. 2005. С. 55.

173. Парфенчик А.А. Использование социальных сетей в государственном управлении // Вопросы государственного и муниципального управления. 2017. №2. С. 186-200.

174. Певцова Е.А. Экстремистские проявления в поведении молодежи в период правовых реформ и кризисных явлений в государстве: проблемы профилактики // Российская юстиция. 2009. №7. С. 13-22.

175. Петрянин А.В. Противодействие преступлениям экстремистской направленности: уголовно-правовой и криминологический аспекты. Дисс. … д. ю. н. М., 2014. С. 380.

176. Печенев В. О национальной и региональной политике в федеративной России // Этнополис. 1994. №1. С. 74-87.

177. Права человека и межнациональные отношения / Отв. ред. Е.А. Лукашева. Москва: РАН, 1994. 131 с.

178. Профилактика экстремизма в молодежной среде: информационно-методический сборник. Иркутск, 2020. 131 с.

179. Профилактика экстремизма в молодежной среде: учебное пособие для вузов / А.В. Мартыненко [и др.]; под общ. ред. А.В. Мартыненко. Москва: Издательство Юрайт, 2020. 221 с. (Высшее образование). – ISBN 978-5-534-04849-0. – Текст: электронный // ЭБС Юрайт [сайт]. – URL: https://urait.ru/bcode/454111

180. Рагузин В.Н. Роль религиозного фактора в межнациональных отношениях. М.: Изд-во РАГС, 1998. 102 с.

181. Распов Н.П. Социально-политическая стабильность регион. субъекта РФ // Полис. 1999. №3. С. 93.

182. Региональное политическое лидерство и современность России: институциональный аспект // ОНС. 2000. №1.

183. Роль и значение СМИ в освещении национальной политики и межнациональных отношений в регионе // Этнопанорама. 2000. №2.

184. Российский федерализм: опыт становления и стратегия перспектив / Под ред. Абдулатипова Р.Г. М.: РАГС, 1998. 228 с.

185. Россия как многонациональная общность и перспективы

межэтнического согласия. М.: АЦ «Российские исследования», 1994. 33 с.

186. Русская нация: историческое прошлое и проблемы возрождения. М., 1995. 222 с.

187. Рябинков А.Г., Рудаков А.Б. Информационно-психологические операции в борьбе с терроризмом и экстремизмом: Учебно-метод. пособие / Под общ. ред. Н.А. Гудкова. Домодедово, 2004. С. 23-25.

188. Семенов В.Е. Дисфункциональность современных российских средств массовой коммуникации // Социальные коммуникации и информация: исследование, образование, практика. Тезисы межвузовской науч.-практ. конф. СПб., 1999. С. 33-34.

189. Семенов В.Е. Современные российские СМИ как негативный фактор социализации молодежи // Экстремизм и СМИ... СПб., 2006. С. 86.

190. Сигарев А.В. Правовое регулирование противодействия экстремизму: курс лекций / А.В. Сигарев; СИУ-филиал РАНХиГС. Новосибирск: Изд-во СибАГС, 2015. С. 96-98.

191. Сикевич З.В. Национальное самосознание русских. М.: Механик, 1996. 204 с.

192. Совет по правам человека. / [Электронный ресурс] // Режим доступа http://molgvardia.ru/nextday/2016/12/09/89799

193. Современный политический экстремизм: понятие, истоки, причины, идеология, проблемы, организации, практика, профилактика и противодействие / Рук. авт. колл. А.-Н.З. Дибиров, Г.К. Сафаралиев. Махачкала, 2009. С. 534-535.

194. Социокультурные особенности молодежного экстремизма: монография / А.Р. Тузиков, Р.И. Зинурова, Э.Б. Гаязова, С.А. Алексеев. Казань: Казанский национальный исследовательский технологический университет, 2015. 188 с. – ISBN 978-5-7882-1863-2. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/63999.html

195. Статус малочисленных народов России (правовые акты и документы). М., 1994. 488 с.

196. Сухонос С.И. Россия в XXI веке. Проблемы национального самосознания. М.: Агар, 1997. 186 с.

197. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. №2. 2018. С. 5-17.

198. Терроризм: история и современность / Кофман Б.И., Миронов С.Н., Сафаров А.А., Сафиуллин Н.Х. Казань, 2002. С. 92.

199. Татарова С.П. Возможности средств массовой информации в профилактике экстремизма // Экстремизм и СМИ... СПб., 2006. С. 182.

200. Тишков В.А. Этнология и политика. М.: Наука, 2001. 240 с.

201. Тишков В.А. Программа «Поддержка межэтнического и религиозного согласия в Приволжском федеральном округе» // Этнопанорама. 2001. №4.

202. Тишков В.А. Институты гражданского общества и миротворчество // Российский Кавказ. М., 2007.

203. Толерантность и согласие: материалы Международной конференции «Толерантность, взаимопонимание и согласие. Якутск. Июнь 1995» / Под ред. В.А. Тишкова. М., 1997. 307 с.

204. Тойнби А. Проблемы истории и теории мировой культуры. М., 1974. 376 с.

205. Томалинцев В.Н. Оценка российской молодежью современных средств массовой информации с позиций социального здоровья // Актуальные проблемы исследования социального здоровья молодежи. Ч. II: Информационно-аналитические материалы / Под ред. Р.А. Зобова. СПб., 2005. С. 46.

206. Туманян О.В. Современные СМИ как фактор влияния на агрессивное и экстремистское поведение молодых // Актуальные вопросы исследования и профилактики экстремизма. Мат-лы Межд. науч.-практ. конф. / Под ред. А.А. Козлова. СПб., 2004. С. 107.

207. Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности // Юридический мир. 2008. №6. С. 26.

208. Филиппов В.Р. Национально-культурная автономия в контексте совершенствования законодательства // Этнографическое обозрение. 2000. №3. С. 55.

209. Халин В.Г., Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы,

угрозы и риски // Управленческое консультирование. 2018. №10. С. 47.

210. Ханстантинов В.А. Культура межнационального общения: сущность, тенденции развития: Дисс… канд. фил. наук. М., 1992. 172 с.

211. Хачирти А.К. Аланика – культура и цивилизация (историко-культурологическое исследование-эссе). В 3-х кн. Кн. 3. Владикавказ, 2009. 398 с.

212. Цалиев А.М. О борьбе с терроризмом, как одной из форм экстремизма // Профилактика экстремизма и терроризма на национальной и религиозной почве. Сборник докладов научно-практической конференции. Владикавказ, 2019. С. 23-35.

213. Цалиев А.М. Актуальные проблемы преступлений экстремистской направленности: состояние, социальная опасность, причины, меры противодействия // VII Международный молодежный юридический форум «Экстремизму – отпор». Сборник научных статей материалов Международной научно-практической конференции / Под ред. Кокоевой Л.Т., Цалиева А.М. 2019. С. 90-110.

214. Цалиев А.М. Совершенствование законодательства и практики его применения как необходимое условие противодействия преступлениям террористического характера // Актуальные проблемы противодействия экстремизму: Материалы Международной научно-практической конференции / Северо-Кавказский горно-металлургический институт (государственный технологический университет). 2018. С. 49-62.

215. Цалиев А.М. О совершенствовании конституционно-правовых основ противодействия экстремизму // Актуальные проблемы противодействия экстремизму: Материалы Международной научно-практической конференции / Северо-Кавказский горно-металлургический институт (государственный технологический университет). 2018. С. 7-21.

216. Цуциев А.А. Осетино-ингушский конфликт (1992- …): его предыстория и факторы развития. М.,1998. 178 с.

217. Чаннов С.Е. Большие данные в государственном управлении: возможности и угрозы // Журнал российского права. №10. 2018. С. 116.

218. Чеджемов С.Р. Правовая культура как фактор противодействия распространению идеологии экстремизма и терроризма среди молодежи (на материалах Северного Кавказа) // Противодействие распространению идеологии экстремизма и терроризма среди молодежи: Материалы Межрегиональной научно-практической конференции по профилактике экстремизма. 2017. С. 249-256.

219. Чеджемов С.Р. Правовое воспитание в деле противодействия экстремизму // Профилактика экстремизма и терроризма на национальной и религиозной почве: Сборник докладов научно-практической конференции. Владикавказ, 2019. С. 36-50.

220. Чичановский А.А. В дружбе народов единство России. Материалы 1 съезда Ассамблеи народов России. М.: Славянский диалог, 1999. 159 с.

221. Швецов А.Н. Государственная политика региональной информатизации: соотношение централизации и местной самостоятельности // Проблемный анализ и государственно-управленческое проектирование. №3. 2013. С. 7.

222. Шипилова Н.Н. Региональные этнополитические конфликты: технологии продуцирования и регулирования: Автореф. дисс... канд. полит. наук. Ростов-на-Дону, 2005.

223. Щербина Е.А. Этническая конфликтология: региональный аспект. Черкесск, 2010. 200 с.

224. Экстремизм в среде петербургской молодежи: анализ и проблемы профилактики / Под ред. А.А. Козлова. СПб., 2003. С. 169.

225. Этнические проблемы современности. Вып. 4. Ставрополь: Изд-во СГУ, 1999. 176 с.

226. Этничность и власть в полиэтничных государствах: Материалы Международной конференции. М.: Наука, 1994. 320 с.

227. Этнополитологическое исследование. М., 2000. 212 с.

228. Явчуновская Р.А. Современные социально-политические проблемы стабильности полиэтничного мира: Дисс… докт. полит. наук. М., 1998. 356 с.

229. Ясавеев И.Г. Конструирование социальных проблем средствами массовой коммуникации. Казань, 2004. С. 149.

ПРИЛОЖЕНИЯ

Приложение 1

Указом Президента
Российской Федерации
от 9 мая 2017 г. №203

СТРАТЕГИЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2030 ГОДЫ

I. Общие положения

1. Настоящая Стратегия определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

2. Правовую основу настоящей Стратегии составляют Конституция Российской Федерации, Федеральный закон от 28 июня 2014 г. №172-ФЗ «О стратегическом планировании в Российской Федерации», другие федеральные законы, Стратегия национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации, утвержденные Президентом Российской Федерации, иные нормативные правовые акты Российской Федерации, определяющие направления применения информационных и коммуникационных технологий в Российской Федерации.

3. Основными принципами настоящей Стратегии являются:

а) обеспечение прав граждан на доступ к информации;

б) обеспечение свободы выбора средств получения знаний при работе с информацией;

в) сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;

г) приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;

д) обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;

е) обеспечение государственной защиты интересов российских граждан в информационной сфере.

4. В настоящей Стратегии используются следующие основные понятия:

а) безопасные программное обеспечение и сервис – программное обеспечение и сервис, сертифицированные на соответствие требованиям к информационной безопасности, устанавливаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, или федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации;

б) индустриальный интернет – концепция построения информационных и коммуникационных инфраструктур на основе подключения к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, а также интеграции данных программно-аппаратных средств между собой без участия человека;

в) интернет вещей – концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека;

г) информационное общество – общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан;

д) информационное пространство – совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информацион-

ных систем и необходимой информационной инфраструктуры;

е) инфраструктура электронного правительства – совокупность размещенных на территории Российской Федерации государственных информационных систем, программно-аппаратных средств и сетей связи, обеспечивающих при оказании услуг и осуществлении функций в электронной форме взаимодействие органов государственной власти Российской Федерации, органов местного самоуправления, граждан и юридических лиц;

ж) критическая информационная инфраструктура Российской Федерации (далее – критическая информационная инфраструктура) – совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой;

з) Национальная электронная библиотека – федеральная государственная информационная система, представляющая собой совокупность документов и сведений в электронной форме (объекты исторического, научного и культурного достояния народов Российской Федерации), доступ к которым предоставляется с использованием сети «Интернет»;

и) облачные вычисления – информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети «Интернет» к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера;

к) обработка больших объемов данных – совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время;

л) общество знаний – общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение до-

стоверной информации с учетом стратегических национальных приоритетов Российской Федерации;

м) объекты критической информационной инфраструктуры – информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности;

н) сети связи нового поколения – технологические системы, предназначенные для подключения к сети «Интернет» пятого поколения в целях использования в устройствах интернета вещей и индустриального интернета;

о) технологически независимые программное обеспечение и сервис – программное обеспечение и сервис, которые могут быть использованы на всей территории Российской Федерации, обеспечены гарантийной и технической поддержкой российских организаций, не имеют принудительного обновления и управления из-за рубежа, модернизация которых осуществляется российскими организациями на территории Российской Федерации и которые не осуществляют несанкционированную передачу информации, в том числе технологической;

п) туманные вычисления – информационно-технологическая модель системного уровня для расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании (компьютеры, мобильные устройства, датчики, смарт-узлы и другое) в сети, а не в «облаке»;

р) цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг;

с) экосистема цифровой экономики – партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан.

II. Россия в современном информационном обществе

5. Международные принципы создания информационного общества и подходы к его созданию определены Окинавской хартией глобального информационного общества (2000 год), Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003 год), Планом действий Тунисского обязательства (2005 год).

6. Первым стратегическим документом, определившим направления развития информационного общества в России, стала Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом Российской Федерации. Она положила начало интенсивному использованию органами государственной власти Российской Федерации, бизнесом и гражданами информационных и коммуникационных технологий.

7. Электронные средства массовой информации, информационные системы, социальные сети, доступ, к которым осуществляется с использованием сети «Интернет», стали частью повседневной жизни россиян. Пользователями российского сегмента сети «Интернет» в 2016 году стали более 80 млн. человек.

8. В России информационное общество характеризуется широким распространением и доступностью мобильных устройств (в среднем на одного россиянина приходится два абонентских номера мобильной связи), а также беспроводных технологий, сетей связи. Создана система предоставления государственных и муниципальных услуг в электронной форме, к которой подключились более 34 млн. россиян. Граждане имеют возможность направить в электронной форме индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления.

9. В России с 2014 года осуществляется подключение населенных пунктов с населением от 250 до 500 человек к сети «Ин-

тернет», в результате чего 5 млн. граждан России, проживающих почти в 14 тыс. таких малонаселенных пунктов, получат доступ к сети «Интернет».

10. Информационные и коммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики. Объем реализации товаров и услуг россиянам с использованием сети «Интернет» в 2015 году достиг эквивалента 2,3 процента валового внутреннего продукта и имеет тенденцию к росту.

11. Информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

12. В России наряду с задачей обеспечения всеобщего доступа к информационным и коммуникационным технологиям актуальной является проблема интенсификации использования самих технологий. Технологии, созданные на основе передовых знаний (нано- и биотехнологии, оптические технологии, искусственный интеллект, альтернативные источники энергии), становятся доступными.

13. Развитие технологий сбора и анализа данных, обмена ими, управления производственными процессами осуществляется на основе внедрения когнитивных технологий, их конвергенции с нано- и биотехнологиями. Значительное увеличение объема данных, источниками и средствами распространения которых являются промышленные и социальные объекты, различные электронные устройства, приводит к формированию новых технологий. Повсеместное применение таких технологий способствует развитию нового этапа экономики – цифровой экономики и образованию ее экосистемы.

14. Главным способом обеспечения эффективности цифровой экономики становится внедрение технологии обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг.

15. Конкурентным преимуществом на мировом рынке обладают государства, отрасли экономики которых основываются на технологиях анализа больших объемов данных. Такие технологии

активно используются в России, но они основаны на зарубежных разработках. Отечественные аналоги в настоящее время отсутствуют. Повсеместное внедрение иностранных информационных и коммуникационных технологий, в том числе на объектах критической информационной инфраструктуры, усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной сфере. С использованием сети «Интернет» все чаще совершаются компьютерные атаки на государственные и частные информационные ресурсы, на объекты критической информационной инфраструктуры.

16. Темпы развития технологий, создания, обработки и распространения информации значительно превысили возможности большинства людей в освоении и применении знаний. Смещение акцентов в восприятии окружающего мира, особенно в сети «Интернет», с научного, образовательного и культурного на развлекательно-справочный сформировало новую модель восприятия – так называемое клиповое мышление, характерной особенностью которого является массовое поверхностное восприятие информации. Такая форма освоения информации упрощает влияние на взгляды и предпочтения людей, способствует формированию навязанных моделей поведения, что дает преимущество в достижении экономических и политических целей тем государствам и организациям, которым принадлежат технологии распространения информации.

17. Международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети «Интернет», не установлены. Большинство государств вынуждены «на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам.

18. Усилия многих государств направлены на приоритетное развитие национальной информационной инфраструктуры в ущерб формированию и распространению знаний, что не в полной мере соответствует целям, продекларированным на Всемирной встрече на высшем уровне по вопросам информационного общества, проходившей в Женеве в 2003 году.

19. Российское общество заинтересовано в получении информации, соответствующей высокому интеллектуальному и культурному уровню развития граждан России.

III. Цель настоящей Стратегии и стратегические национальные приоритеты Российской Федерации при развитии информационного общества

20. Целью настоящей Стратегии является создание условий для формирования в Российской Федерации общества знаний.

21. Настоящая Стратегия призвана способствовать обеспечению следующих национальных интересов:

а) развитие человеческого потенциала;

б) обеспечение безопасности граждан и государства;

в) повышение роли России в мировом гуманитарном и культурном пространстве;

г) развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления;

д) повышение эффективности государственного управления, развитие экономики и социальной сферы;

е) формирование цифровой экономики.

22. Обеспечение национальных интересов при развитии информационного общества осуществляется путем реализации следующих приоритетов:

а) формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

б) развитие информационной и коммуникационной инфраструктуры Российской Федерации;

в) создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне;

г) формирование новой технологической основы для развития экономики и социальной сферы;

д) обеспечение национальных интересов в области цифровой экономики.

23. В целях развития информационного общества государством создаются условия для формирования пространства знаний и предоставления доступа к нему, совершенствования механизмов распространения знаний, их применения на практике в интересах личности, общества и государства.

Формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений

24. Целями формирования информационного пространства, основанного на знаниях (далее – информационное пространство знаний), являются обеспечение прав граждан на объективную, достоверную, безопасную информацию и создание условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора.

25. Формирование информационного пространства знаний осуществляется путем развития науки, реализации образовательных и просветительских проектов, создания для граждан общедоступной системы взаимоувязанных знаний и представлений, обеспечения безопасной информационной среды для детей, продвижения русского языка в мире, поддержки традиционных (отличных от доступных с использованием сети «Интернет») форм распространения знаний.

26. Для формирования информационного пространства знаний необходимо:

а) проводить мероприятия в области духовно-нравственного воспитания граждан;

б) реализовать просветительские проекты, направленные на обеспечение доступа к знаниям, достижениям современной науки и культуры;

в) проводить мероприятия по сохранению культуры и общероссийской идентичности народов Российской Федерации;

г) сформировать безопасную информационную среду на основе популяризации информационных ресурсов, способствующих распространению традиционных российских духовно-нравственных ценностей;

д) усовершенствовать механизмы обмена знаниями;

е) обеспечить формирование Национальной электронной библиотеки и иных государственных информационных систем, включающих в себя объекты исторического, научного и культурного наследия народов Российской Федерации, а также доступ к ним максимально широкого круга пользователей;

ж) обеспечить условия для научно-технического творчества, включая создание площадок для самореализации представителей образовательных и научных организаций;

з) обеспечить совершенствование дополнительного образования для привлечения детей к занятиям научными изысканиями и творчеством, развития их способности решать нестандартные задачи;

и) использовать и развивать различные образовательные технологии, в том числе дистанционные, электронное обучение, при реализации образовательных программ;

к) создать условия для популяризации русской культуры и науки за рубежом, в том числе для противодействия попыткам искажения и фальсификации исторических и других фактов;

л) установить устойчивые культурные и образовательные связи с проживающими за рубежом соотечественниками, иностранными гражданами и лицами без гражданства, являющимися носителями русского языка, в том числе на основе информационных и коммуникационных технологий;

м) осуществлять разработку и реализацию партнерских программ образовательных организаций высшего образования и российских высокотехнологичных организаций, в том числе по вопросу совершенствования образовательных программ;

н) формировать и развивать правосознание граждан и их ответственное отношение к использованию информационных технологий, в том числе потребительскую и пользовательскую культуру;

о) обеспечить создание и развитие систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления;

п) совершенствовать механизмы ограничения доступа к информации, распространение которой в Российской Федерации запрещено федеральным законом, и ее удаления;

р) совершенствовать механизмы законодательного регулирования деятельности средств массовой информации, а также средств обеспечения доступа к информации, которые по многим признакам могут быть отнесены к средствам массовой информации, но не являются таковыми (интернет-телевидение, новостные агрегаторы, социальные сети, сайты в сети «Интернет», мессенджеры);

с) принять меры по эффективному использованию современных информационных платформ для распространения достоверной и качественной информации российского производства;

т) обеспечить насыщение рынка доступными, качественными и легальными медиапродуктами и сервисами российского производства;

у) принять меры поддержки традиционных средств распространения информации (радио-, телевещание, печатные средства массовой информации, библиотеки).

Развитие информационной и коммуникационной инфраструктуры Российской Федерации

27. Целью развития информационной и коммуникационной инфраструктуры Российской Федерации (далее – информационная инфраструктура Российской Федерации) является обеспечение свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее создания и распространения.

28. Для недопущения подмены, искажения, блокирования, удаления, снятия с каналов связи и иных манипуляций с информацией развитие информационной инфраструктуры Российской Федерации осуществляется:

а) на уровне программного обеспечения и сервисов, предоставляемых с использованием сети «Интернет»;

б) на уровне информационных систем и центров обработки данных;

в) на уровне сетей связи (линии и средства связи, инфраструктура российского сегмента сети «Интернет», технологические и выделенные сети связи, сети и оборудование интернета вещей).

29. Для устойчивого функционирования информационной инфраструктуры Российской Федерации необходимо:

а) обеспечить единство государственного регулирования, централизованные мониторинг и управление функционированием информационной инфраструктуры Российской Федерации на уровне информационных систем и центров обработки данных, а также на уровне сетей связи;

б) обеспечить поэтапный переход государственных органов и органов местного самоуправления к использованию инфраструктуры электронного правительства, входящей в информационную инфраструктуру Российской Федерации;

в) обеспечить использование российских криптоалгоритмов и средств шифрования при электронном взаимодействии федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления между собой, а также с гражданами и организациями;

г) осуществить скоординированные действия, направленные на подключение объектов к информационной инфраструктуре Российской Федерации;

д) заменить импортное оборудование, программное обеспечение и электронную компонентную базу российскими аналогами, обеспечить технологическую и производственную независимость и информационную безопасность;

е) обеспечить комплексную защиту информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры;

ж) проводить непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них;

з) обеспечить единство сетей электросвязи Российской Федерации, в том числе развитие и функционирование сетей связи государственных органов и органов местного самоуправления, а также интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка.

30. Для предоставления безопасных и технологически независимых программного обеспечения и сервисов необходимо:

а) создать российское общесистемное и прикладное программное обеспечение, телекоммуникационное оборудование и пользовательские устройства для широкого использования гражданами, субъектами малого, среднего и крупного предпринимательства, государственными органами и органами местного самоуправления, в том числе на основе обработки больших объемов данных, применения облачных технологий и интернета вещей;

б) создать встроенные средства защиты информации для применения в российских информационных и коммуникационных технологиях;

в) обеспечить использование российских информационных и коммуникационных технологий в органах государственной власти Российской Федерации, компаниях с государственным участием, органах местного самоуправления;

г) создать справедливые условия ведения предпринимательской деятельности для российских разработчиков.

31. Для защиты данных в Российской Федерации необходимо:

а) совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих технологий и интересам общества;

б) обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну;

в) упорядочить алгоритмы обработки данных и доступа к таким данным;

г) обеспечить обработку данных на российских серверах при электронном взаимодействии лиц, находящихся на территории

Российской Федерации, а также передачу таких данных на территории Российской Федерации с использованием сетей связи российских операторов;

д) обеспечить государственное регулирование и координацию действий при создании и ведении информационных ресурсов в Российской Федерации в целях соблюдения принципа разумной достаточности при обработке данных;

е) проводить мероприятия по противодействию незаконным обработке и сбору сведений о гражданах, в том числе персональных данных граждан, на территории Российской Федерации неуполномоченными и неустановленными лицами, а также используемым ими техническим средствам.

32. Для эффективного управления сетями связи Российской Федерации, обеспечения их целостности, единства, устойчивого функционирования и безопасности работы необходимо:

а) создать централизованную систему мониторинга и управления единой сетью электросвязи Российской Федерации;

б) создать системы, обеспечивающие возможность устойчивого, безопасного и независимого функционирования российского сегмента сети «Интернет»;

в) обеспечить надежность и доступность услуг связи в России, в том числе в сельской местности и труднодоступных населенных пунктах;

г) проводить работу по созданию государственными органами и организациями условий для расширения использования в сетях связи телекоммуникационного оборудования и программного обеспечения, исключающих возможность несанкционированного управления ими и не содержащих составных частей и элементов, замена, ремонт или производство которых в течение срока службы невозможны на территории Российской Федерации;

д) поддерживать инфраструктуру традиционных услуг связи (почтовая связь, электросвязь).

33. Для обеспечения функционирования социальных, экономических и управленческих систем с использованием российского сегмента сети «Интернет» необходимо:

а) принять меры по обеспечению устойчивого функционирования российского сегмента сети «Интернет»;

б) реализовывать государственную политику в части, касающейся государственного управления инфраструктурой российского сегмента сети «Интернет»;

в) выработать технические и законодательные меры по предотвращению нарушений работы сети «Интернет» и отдельных ее ресурсов на территории Российской Федерации в результате целенаправленных действий.

34. Для развития сети «Интернет» и информационной инфраструктуры Российской Федерации необходимо проводить следующие мероприятия на международном уровне:

а) отстаивать суверенное право государства определять информационную, технологическую и экономическую политику в национальном сегменте сети «Интернет»;

б) вести работу, направленную против использования сети «Интернет» в военных целях;

в) развивать гуманитарное значение сети «Интернет»;

г) разрабатывать нормы международно-правового регулирования, касающиеся безопасного и устойчивого функционирования и развития сети «Интернет», включая вопросы юрисдикции и определения субъектов правоотношений, на основе равноправного участия членов мирового сообщества в управлении глобальной информационной сетью и ее ресурсами с учетом уникальности данной сферы;

д) создать новые механизмы партнерства, призванные с участием всех институтов общества выработать систему доверия в сети «Интернет», гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации и исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети «Интернет»;

е) осуществить интеграцию российских стандартов в сфере информационных и коммуникационных технологий в соответствующие международные стандарты, а также обеспечить гармонизацию межгосударственной и национальной систем стандартов в данной сфере.

Создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне

35. Создание российских информационных и коммуникационных технологий осуществляется в целях получения государством и гражданами новых технологических преимуществ, использования и обработки информации, доступа к ней, получения знаний, формирования новых рынков и обеспечения лидерства на них.

36. Основными направлениями развития российских информационных и коммуникационных технологий, перечень которых может быть изменен по мере появления новых технологий, являются:

а) конвергенция сетей связи и создание сетей связи нового поколения;

б) обработка больших объемов данных;

в) искусственный интеллект;

г) доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере;

д) облачные и туманные вычисления;

е) интернет вещей и индустриальный интернет;

ж) робототехника и биотехнологии;

з) радиотехника и электронная компонентная база;

и) информационная безопасность.

37. Ключевыми направлениями повышения конкурентоспособности российских информационных и коммуникационных технологий являются:

а) развитие науки, техники, технологий;

б) подготовка квалифицированных кадров в сфере информационных и коммуникационных технологий;

в) внедрение отечественных информационных технологий, формирование представления о внедрении инноваций как о приоритетном пути технологического развития;

г) стимулирование создания российских организаций, осуществляющих деятельность, направленную на развитие всего спектра сервисов цифровой экономики, и способных лидировать

на внутреннем и внешнем рынках (экосистемы цифровой экономики);

д) обеспечение трансфера иностранных технологий и применение лучшего зарубежного опыта в сфере информационных технологий;

е) сотрудничество российских и иностранных организаций в сфере информационных и коммуникационных технологий на паритетных началах.

38. При создании российских информационных и коммуникационных технологий необходимо:

а) обеспечить актуальность научно-исследовательских приоритетов и последовательное развитие прикладных решений на основании передовых фундаментальных научных исследований;

б) расширять возможности многостороннего и двустороннего научно-технического сотрудничества в сфере информационных и коммуникационных технологий, укреплять исследовательский потенциал и информационный обмен между государствами;

в) проводить на региональном и международном уровнях мероприятия, направленные на продвижение российских товаров и услуг, в интересах российских организаций, развивающих и внедряющих отечественные информационные и коммуникационные технологии;

г) осуществлять стимулирование фундаментальных и прикладных научных исследований в сфере информационных и коммуникационных технологий, выполняемых научно-исследовательскими организациями, а также разработку инновационного высокотехнологичного оборудования в указанной сфере;

д) оказывать государственную поддержку в части, касающейся защиты интеллектуальной собственности российских правообладателей и совместного использования знаний, в том числе за рубежом;

е) разрабатывать и продвигать российские подходы и стандарты, позволяющие обеспечить конкурентоспособность приоритетных отечественных технологий, подходов и стандартов на международном уровне;

ж) обеспечивать экспорт российских информационных и коммуникационных технологий;

з) регулировать импорт иностранных информационных и коммуникационных технологий с учетом международных обязательств Российской Федерации;

и) создать условия для технологического преимущества бизнес-моделей российских организаций в глобальной цифровой экономике.

Формирование новой технологической основы для развития экономики и социальной сферы

39. Целью создания новой технологической основы для развития экономики и социальной сферы является повышение качества жизни граждан на основе широкого применения отечественных информационных и коммуникационных технологий, направленных на повышение производительности труда, эффективности производства, стимулирование экономического роста, привлечение инвестиций в производство инновационных технологий, повышение конкурентоспособности Российской Федерации на мировых рынках, обеспечение ее устойчивого и сбалансированного долгосрочного развития.

40. Основными задачами применения информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства являются:

а) реализация проектов по повышению доступности качественных медицинских услуг и медицинских товаров;

б) создание различных технологических платформ для дистанционного обучения в целях повышения доступности качественных образовательных услуг;

в) совершенствование механизмов предоставления финансовых услуг в электронной форме и обеспечение их информационной безопасности;

г) стимулирование российских организаций в целях обеспечения работникам условий для дистанционной занятости;

д) развитие технологий электронного взаимодействия граждан, организаций, государственных органов, органов местного самоуправления наряду с сохранением возможности взаимодей-

ствия граждан с указанными организациями и органами без применения информационных технологий;

е) применение в органах государственной власти Российской Федерации новых технологий, обеспечивающих повышение качества государственного управления;

ж) совершенствование механизмов электронной демократии;

з) обеспечение возможности использования информационных и коммуникационных технологий при проведении опросов и переписи населения;

и) создание основанных на информационных и коммуникационных технологиях систем управления и мониторинга во всех сферах общественной жизни.

41. Основными задачами применения информационных технологий в сфере взаимодействия государства и бизнеса, формирования новой технологической основы в экономике являются:

а) своевременное распространение достоверных сведений о различных аспектах социально-экономического развития, в том числе данных официального статистического учета;

б) создание условий для развития электронного взаимодействия участников экономической деятельности, в том числе финансовых организаций и государственных органов;

в) использование инфраструктуры электронного правительства для оказания государственных, а также востребованных гражданами коммерческих и некоммерческих услуг;

г) продвижение проектов по внедрению электронного документооборота в организациях, создание условий для повышения доверия к электронным документам, осуществление в электронной форме идентификации и аутентификации участников правоотношений;

д) обеспечение доступности электронных форм коммерческих отношений для предприятий малого и среднего бизнеса;

е) сокращение административной нагрузки на субъекты хозяйственной деятельности вследствие использования информационных и коммуникационных технологий при проведении проверок органами государственного и муниципального контроля (надзора) и при сборе данных официального статистического учета;

ж) создание электронной системы представления субъектами хозяйственной деятельности отчетности в органы государственной власти Российской Федерации и органы местного самоуправления, а также сохранение возможности представления документов традиционным способом;

з) внедрение систем повышения эффективности труда в государственных и коммерческих организациях;

и) разработка мер, направленных на внедрение в российских организациях, в том числе в организациях жилищно-коммунального хозяйства и сельскохозяйственных организациях, российских информационных технологий, включая технологии обработки больших объемов данных, облачных вычислений, интернета вещей;

к) обеспечение дистанционного доступа к банковским услугам, в том числе внедрение единых подходов к проверке сведений, предоставляемых при банковском обслуживании, в электронной форме;

л) развитие трансграничного информационного взаимодействия, в том числе обеспечение трансграничного пространства доверия к электронной подписи.

Обеспечение национальных интересов в области цифровой экономики

42. Национальными интересами в области цифровой экономики являются:

а) формирование новых рынков, основанных на использовании информационных и коммуникационных технологий, и обеспечение лидерства на этих рынках за счет эффективного применения знаний, развития российской экосистемы цифровой экономики;

б) укрепление российской экономики, в том числе тех ее отраслей, в которых развитие бизнеса с использованием информационных и коммуникационных технологий предоставит конкурентные преимущества российским организациям, обеспечит эффективность производства и рост производительности труда;

в) увеличение за счет применения новых технологий объема несырьевого российского экспорта, в первую очередь товаров и услуг, пользующихся спросом у иностранных потребителей;

г) повышение конкурентоспособности российских высокотехнологичных организаций на международном рынке;

д) обеспечение технологической независимости и безопасности инфраструктуры, используемой для продажи товаров и оказания услуг российским гражданам и организациям;

е) защита граждан от контрафактной и некачественной продукции;

ж) обеспечение правомерного использования персональных данных, информации, источником которой являются объекты промышленной, транспортной инфраструктур, инфраструктуры связи, а также данных, полученных из государственных информационных систем;

з) защита интересов российских граждан, обеспечение их занятости (развитие цифровой экономики не должно ущемлять интересы граждан);

и) сохранение существующих в традиционных отраслях экономики технологий и способов производства товаров и оказания услуг;

к) обеспечение защиты интересов российских организаций, реализующих свою продукцию на традиционных (неэлектронных) рынках;

л) совершенствование антимонопольного законодательства, в том числе при предоставлении программного обеспечения, товаров и услуг с использованием сети «Интернет» лицам, находящимся на территории Российской Федерации;

м) выполнение требований законодательства Российской Федерации иностранными участниками российского рынка наравне с российскими организациями;

н) развитие торговых и экономических связей со стратегическими партнерами Российской Федерации, в том числе в рамках Евразийского экономического союза (ЕАЭС).

43. В процессе реализации национальных интересов в области цифровой экономики необходимо:

а) создать условия для развития крупных российских организаций в сфере информационных и коммуникационных технологий (экосистемы цифровой экономики);

б) обеспечить создание кросс-отраслевых консорциумов в сфере цифровой экономики на базе крупнейших российских интернет-компаний, банков, операторов связи (в том числе почтовой), операторов платежных систем, участников финансового рынка, государственных компаний и корпораций;

в) обеспечить поддержку выхода российских организаций на зарубежные рынки товаров и услуг;

г) обеспечить соблюдение антимонопольного законодательства при ведении бизнеса российскими и иностранными организациями в сфере цифровой экономики, а также равные налоговые условия;

д) создать условия для локализации иностранными организациями на территории Российской Федерации процессов производства и использования продукции в сфере информационных и коммуникационных технологий;

е) установить правила недискриминационного доступа к товарам и услугам, производимым или реализуемым российскими организациями;

ж) вносить в законодательство Российской Федерации изменения, направленные на обеспечение соответствия нормативно-правового регулирования темпам развития цифровой экономики и устранение административных барьеров;

з) обеспечить участие российских государственных органов и организаций в разработке международных договоров и иных документов в сфере цифровой экономики;

и) законодательно регламентировать доступ организаций к данным о гражданах и юридических лицах, в том числе содержащимся в государственных информационных системах, порядок обработки данных, а также порядок государственной защиты персональных данных граждан на территории Российской Федерации;

к) обеспечить защиту данных путем использования российских информационных и коммуникационных технологий в области защиты информации;

л) обеспечить защиту данных от несанкционированной и незаконной трансграничной передачи иностранным организациям;

м) развивать центры обработки данных, технические средства

по обработке данных на территории Российской Федерации на основе российского программного обеспечения и оборудования;

н) обеспечить с использованием российской национальной платежной системы и элементов информационной инфраструктуры Российской Федерации безопасность проведения в сети «Интернет» финансовых операций, прозрачность трансграничных платежей (идентификация плательщика, получателя, назначение платежа), в том числе за счет применения сертифицированных средств защиты информации;

о) обеспечить создание российской платежной и логистической инфраструктуры интернет-торговли;

п) применять меры таможенного контроля в отношении товаров, заказанных с использованием сети «Интернет»;

р) обеспечить сертификацию и лицензирование товаров и услуг, ввозимых в Российскую Федерацию, в том числе приобретаемых с использованием сети «Интернет»;

с) определить в рамках ЕАЭС правила доступа товаров и услуг иностранных организаций на внутренние рынки государств – членов ЕАЭС, обеспечить интеграцию российской экономики в единое пространство цифровой экономики ЕАЭС;

т) принять меры по ограничению доступа к программному обеспечению, товарам и услугам, предоставляемым с использованием сети «Интернет» на территории Российской Федерации иностранными организациями, допустившими нарушение законодательства Российской Федерации;

у) обеспечить иностранным организациям, оказывающим услуги на территории Российской Федерации, возможность создания своих представительств в России, а также совместных предприятий с крупными российскими организациями на паритетных условиях;

ф) проводить мероприятия по защите прав российских потребителей при продаже товаров с использованием сети «Интернет» и дистанционном оказании услуг;

х) обеспечить создание и функционирование на территории Российской Федерации представительств иностранных организаций для работы с жалобами и обращениями российских граждан и исполнения требований государственных органов.

44. Сотрудничество российских организаций с иностранными организациями в сфере цифровой экономики осуществляется на следующих условиях и принципах:

а) хранение информации об осуществляемой указанными организациями деятельности и обработка данных производятся исключительно на серверах и в базах данных, находящихся на территории Российской Федерации;

б) защита интересов и безопасности российских участников электронной торговли осуществляется с учетом соблюдения требований идентификации, подтверждения достоверности и подлинности используемых документов;

в) обеспечение режима наибольшего благоприятствования (с необходимыми изъятиями) для российских поставщиков и покупателей при доступе к информации о товарах и услугах и при реализации товаров и услуг в режиме электронной торговли на территории Российской Федерации, а также при продвижении товаров на территории иностранных государств при условии соблюдения интересов национальных логистических операторов;

г) осуществление расчетов между участниками электронной торговли через российскую платежную систему.

45. Сотрудничество российских и иностранных организаций в сфере цифровой экономики не предполагает оказание на территории Российской Федерации финансовых услуг иностранными организациями.

IV. Приоритетный сценарий развития информационного общества в России

46. Государство создает благоприятные условия для применения информационных и коммуникационных технологий. Совершенствуются законодательство Российской Федерации, административные процедуры (в том числе в электронной форме) и бизнес-процессы коммерческих организаций.

47. Инвестиции (в том числе бюджетные инвестиции из федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов) осуществляются в определенные государством и обществом приоритетные направления поддержки и раз-

вития информационных и коммуникационных технологий.

48. Привлекаются частные инвестиции в информационную инфраструктуру Российской Федерации.

49. Российские организации создают и совершенствуют прорывные информационные и коммуникационные технологии. Их интересы защищаются государством. Технологии, произведенные в России, востребованы за рубежом.

50. Сформированы национальные технологические платформы онлайн-образования, онлайн-медицины, единая инфраструктура электронного правительства, Национальная электронная библиотека. Граждане осведомлены о преимуществах получения информации, приобретения товаров и получения услуг с использованием сети «Интернет», а также имеют возможность получать финансовые услуги в электронной форме, онлайн-образование, услуги онлайн-медицины, электронных библиотек, государственные и муниципальные услуги.

51. Цифровая экономика оказывает существенное влияние на темпы роста валового внутреннего продукта Российской Федерации.

V. Перечень показателей реализации настоящей Стратегии и этапы ее реализации

52. В целях осуществления мониторинга реализации настоящей Стратегии Правительство Российской Федерации утверждает перечень показателей ее реализации и значения этих показателей, отражающие:

а) оценку развития информационных и коммуникационных технологий в Российской Федерации;

б) оценку развития информационного общества в Российской Федерации;

в) параметры формирования цифровой экономики, оценку ее влияния на темпы роста валового внутреннего продукта Российской Федерации;

г) состояние перехода к использованию организациями наукоемких технологий.

53. Этапы реализации настоящей Стратегии определяются в

плане ее реализации, который разрабатывается и утверждается Правительством Российской Федерации.

54. План реализации настоящей Стратегии включает в себя следующие основные мероприятия:

а) разработка статистического инструментария для оценки реализации настоящей Стратегии и мониторинга достижения значений показателей ее реализации;

б) принятие законодательных и издание иных нормативных правовых актов Российской Федерации, субъектов Российской Федерации, направленных на реализацию настоящей Стратегии;

в) внесение изменений в государственные программы Российской Федерации, государственные программы субъектов Российской Федерации, планы деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, институтов развития, компаний с государственным участием.

VI. Управление реализацией настоящей Стратегии. Источники и механизмы ресурсного обеспечения мероприятий по реализации настоящей Стратегии. Задачи, функции и порядок взаимодействия государственных органов, органов местного самоуправления и организаций при реализации настоящей Стратегии

55. Реализация настоящей Стратегии обеспечивается согласованными действиями следующих государственных органов, органов местного самоуправления и организаций:

а) Правительство Российской Федерации;

б) Администрация Президента Российской Федерации;

в) аппарат Совета Безопасности Российской Федерации;

г) федеральные органы исполнительной власти;

д) Центральный банк Российской Федерации;

е) органы исполнительной власти субъектов Российской Федерации;

ж) органы местного самоуправления;

з) государственные внебюджетные фонды;

и) фонды и институты развития (в соответствии с планом реализации настоящей Стратегии);

к) государственные корпорации, компании с государственным участием и частные компании (в соответствии с планом реализации настоящей Стратегии).

56. Финансовое обеспечение реализации настоящей Стратегии осуществляется за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов, средств государственных внебюджетных фондов и внебюджетных источников, включая средства институтов развития, компаний с государственным участием, государственных корпораций.

57. Согласованное планирование и реализация мероприятий, предусмотренных настоящей Стратегией, осуществляются на основе документов стратегического планирования с использованием механизмов координации мероприятий по обеспечению стратегического управления в сфере развития информационного общества, реализуемых органами государственной власти и органами местного самоуправления.

58. В рамках реализации настоящей Стратегии российские фонды, институты развития, государственные корпорации, компании с государственным участием и частные компании осуществляют инвестиции в сферу информационных и коммуникационных технологий.

59. Мероприятия по реализации настоящей Стратегии учитываются при формировании и корректировке государственных программ Российской Федерации, программ институтов развития, программ субъектов Российской Федерации по созданию и развитию информационного общества.

60. В соответствии с планом реализации настоящей Стратегии в государственные программы вносятся необходимые изменения.

61. План реализации настоящей Стратегии, кроме перечня основных мероприятий по ее реализации, включает в себя задачи и порядок координации деятельности и взаимодействия государственных органов, органов местного самоуправления и организаций при реализации настоящей Стратегии.

62. Федеральные органы исполнительной власти включают в планы своей деятельности мероприятия по реализации настоящей Стратегии.

63. Органы исполнительной власти субъектов Российской Федерации вносят в планы реализации региональных документов стратегического планирования изменения в соответствии с настоящей Стратегией.

64. Оценка эффективности результатов деятельности руководителей федеральных органов исполнительной власти и высших должностных лиц (руководителей высших исполнительных органов государственной власти) субъектов Российской Федерации по реализации настоящей Стратегии проводится ежегодно.

65. Положения настоящей Стратегии и план ее реализации обязательны для выполнения всеми органами государственной власти Российской Федерации и органами местного самоуправления и являются основой для разработки и корректировки соответствующих государственных, ведомственных и региональных программ и планов.

Приложение 2

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О противодействии экстремистской деятельности

Принят Государственной Думой 27 июня 2002 года
Одобрен Советом Федерации 10 июля 2002 года

(В редакции федеральных законов от 27.07.2006 г. №148-ФЗ;
от 27.07.2006 г. №153-ФЗ; от 10.05.2007 г. №71-ФЗ;
от 24.07.2007 г. №211-ФЗ; от 29.04.2008 г. №54-ФЗ;
от 25.12.2012 г. №255-ФЗ; от 02.07.2013 г. №185-ФЗ;
от 28.06.2014 г. №179-ФЗ; от 21.07.2014 г. №236-ФЗ;
от 31.12.2014 г. №505-ФЗ; от 08.03.2015 г. №23-ФЗ;
от 23.11.2015 г. №314-ФЗ)

Настоящим Федеральным законом в целях защиты прав и свобод человека и гражданина, основ конституционного строя, обеспечения целостности и безопасности Российской Федерации определяются правовые и организационные основы противодействия экстремистской деятельности, устанавливается ответственность за ее осуществление.

Статья 1. Основные понятия

Для целей настоящего Федерального закона применяются следующие основные понятия:

1) экстремистская деятельность (экстремизм):

насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

публичное оправдание терроризма и иная террористическая деятельность;

возбуждение социальной, расовой, национальной или религиозной розни;

пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, нацио-

нальной, религиозной или языковой принадлежности или отношения к религии;

нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации;

пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций (В редакции Федерального закона от 25.12.2012 г. №255-ФЗ);

публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг (Пункт в редакции Федерального закона от 24.07.2007 г. №211-ФЗ);

2) экстремистская организация – общественное или религиозное объединение либо иная организация, в отношении которых по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности;

3) экстремистские материалы – предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;

4) символика экстремистской организации – символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности. (Пункт дополнен – Федеральный закон от 25.12.2012 г. №255-ФЗ) (В редакции Федерального закона от 21.07.2014 г. №236-ФЗ) (Статья в редакции Федерального закона от 27.07.2006 г. №148-ФЗ).

Статья 2. Основные принципы противодействия экстремистской деятельности

Противодействие экстремистской деятельности основывается на следующих принципах:

признание, соблюдение и защита прав и свобод человека и гражданина, а равно законных интересов организаций;

законность;

гласность;

приоритет обеспечения безопасности Российской Федерации;

приоритет мер, направленных на предупреждение экстремистской деятельности;

сотрудничество государства с общественными и религиозными объединениями, иными организациями, гражданами в противодействии экстремистской деятельности;

неотвратимость наказания за осуществление экстремистской деятельности.

Статья 3. Основные направления противодействия экстремистской деятельности

Противодействие экстремистской деятельности осуществляется по следующим основным направлениям:

принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности;

выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

Статья 3-1. Особенности применения законодательства Российской Федерации о противодействии экстремистской деятельности в отношении религиозных текстов

Библия, Коран, Танах и Ганджур, их содержание и цитаты из них не могут быть признаны экстремистскими материалами. (Статья дополнена – Федеральный закон от 23.11.2015 г. №314-ФЗ).

Статья 4. Организационные основы противодействия экстремистской деятельности

Президент Российской Федерации:

определяет основные направления государственной политики в области противодействия экстремистской деятельности;

устанавливает компетенцию федеральных органов исполнительной власти, руководство деятельностью которых он осуществляет, по противодействию экстремистской деятельности.

Правительство Российской Федерации:

определяет компетенцию федеральных органов исполнительной власти, руководство деятельностью которых оно осуществляет, в области противодействия экстремистской деятельности;

организует разработку и осуществление мер по предупреждению экстремистской деятельности, минимизацию и (или) ликвидацию последствий ее проявлений;

организует обеспечение деятельности федеральных органов исполнительной власти по противодействию экстремистской деятельности необходимыми силами, средствами и ресурсами.

Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и органы местного самоуправления участвуют в противодействии экстремистской деятельности в пределах своей компетенции.

В целях обеспечения координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления по противодействию экстремистской деятельности по решению Президента Российской Федерации могут формироваться органы в составе представителей федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и иных лиц. Для реализации решений этих органов могут издаваться акты (совместные акты) указанных органов, представители которых входят в состав соответствующего органа. (Статья в редакции Федерального закона от 28.06.2014 г. №179-ФЗ).

Статья 5. Профилактика экстремистской деятельности

В целях противодействия экстремистской деятельности федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в пределах своей компетенции в приоритетном порядке осуществляют профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской деятельности.

Статья 6. Объявление предостережения о недопустимости осуществления экстремистской деятельности

При наличии достаточных и предварительно подтвержденных сведений о готовящихся противоправных действиях, содержащих признаки экстремистской деятельности, и при отсутствии оснований для привлечения к уголовной ответственности Генеральный прокурор Российской Федерации или его заместитель либо подчиненный ему соответствующий прокурор или его заместитель направляет руководителю общественного или религиозного объединения либо руководителю иной организации, а также другим соответствующим лицам предостережение в письменной форме о недопустимости такой деятельности с указанием конкретных оснований объявления предостережения.

В случае невыполнения требований, изложенных в предостережении, лицо, которому было объявлено данное предостережение, может быть привлечено к ответственности в установленном порядке.

Предостережение может быть обжаловано в суде в установленном порядке.

Статья 7. Вынесение предупреждения общественному или религиозному объединению либо иной организации о недопустимости осуществления экстремистской деятельности

Общественному или религиозному объединению либо иной организации в случае выявления фактов, свидетельствующих о наличии в их деятельности, в том числе в деятельности хотя бы одного из их региональных или других структурных подразделе-

ний, признаков экстремизма, выносится предупреждение в письменной форме о недопустимости такой деятельности с указанием конкретных оснований вынесения предупреждения, в том числе допущенных нарушений. В случае, если возможно принять меры по устранению допущенных нарушений, в предупреждении также устанавливается срок для устранения указанных нарушений, составляющий не менее двух месяцев со дня вынесения предупреждения.

Предупреждение общественному или религиозному объединению либо иной организации выносится Генеральным прокурором Российской Федерации или подчиненным ему соответствующим прокурором.

Предупреждение общественному или религиозному объединению может быть вынесено также федеральным органом исполнительной власти, осуществляющим функции в сфере государственной регистрации некоммерческих организаций, общественных объединений и религиозных организаций (далее – федеральный орган государственной регистрации), или его соответствующим территориальным органом. (В редакции Федерального закона от 29.04.2008 г. №54-ФЗ).

Предупреждение может быть обжаловано в суд в установленном порядке.

В случае если предупреждение не было обжаловано в суд в установленном порядке или не признано судом незаконным, а также если в установленный в предупреждении срок соответствующими общественным или религиозным объединением, либо иной организацией, либо их региональным или другим структурным подразделением не устранены допущенные нарушения, послужившие основанием для вынесения предупреждения, либо если в течение двенадцати месяцев со дня вынесения предупреждения выявлены новые факты, свидетельствующие о наличии признаков экстремизма в их деятельности, в установленном настоящим Федеральным законом порядке соответствующие общественное или религиозное объединение либо иная организация подлежит ликвидации, а деятельность общественного или религиозного объединения, не являющегося юридическим лицом, подлежит запрету.

Статья 8. Предупреждение о недопустимости распространения экстремистских материалов через средство массовой информации и осуществления им экстремистской деятельности

В случае распространения через средство массовой информации экстремистских материалов либо выявления фактов, свидетельствующих о наличии в его деятельности признаков экстремизма, учредителю и (или) редакции (главному редактору) данного средства массовой информации уполномоченным государственным органом, осуществившим регистрацию данного средства массовой информации, либо федеральным органом исполнительной власти в сфере печати, телерадиовещания и средств массовых коммуникаций, либо Генеральным прокурором Российской Федерации или подчиненным ему соответствующим прокурором выносится предупреждение в письменной форме о недопустимости таких действий либо такой деятельности с указанием конкретных оснований вынесения предупреждения, в том числе допущенных нарушений. В случае если возможно принять меры по устранению допущенных нарушений, в предупреждении также устанавливается срок для устранения указанных нарушений, составляющий не менее десяти дней со дня вынесения предупреждения.

Предупреждение может быть обжаловано в суд в установленном порядке.

В случае если предупреждение не было обжаловано в суд в установленном порядке или не признано судом незаконным, а также если в установленный в предупреждении срок не приняты меры по устранению допущенных нарушений, послуживших основанием для вынесения предупреждения, либо если повторно в течение двенадцати месяцев со дня вынесения предупреждения выявлены новые факты, свидетельствующие о наличии признаков экстремизма в деятельности средства массовой информации, деятельность соответствующего средства массовой информации подлежит прекращению в установленном настоящим Федеральным законом порядке.

Статья 9. Ответственность общественных и религиозных объединений, иных организаций за осуществление экстремистской деятельности

В Российской Федерации запрещаются создание и деятельность общественных и религиозных объединений, иных организаций, цели или действия которых направлены на осуществление экстремистской деятельности.

В случае, предусмотренном частью четвертой статьи 7 настоящего Федерального закона, либо в случае осуществления общественным или религиозным объединением, либо иной организацией, либо их региональным или другим структурным подразделением экстремистской деятельности, повлекшей за собой нарушение прав и свобод человека и гражданина, причинение вреда личности, здоровью граждан, окружающей среде, общественному порядку, общественной безопасности, собственности, законным экономическим интересам физических и (или) юридических лиц, обществу и государству или создающей реальную угрозу причинения такого вреда, соответствующие общественное или религиозное объединение либо иная организация могут быть ликвидированы, а деятельность соответствующего общественного или религиозного объединения, не являющегося юридическим лицом, может быть запрещена по решению суда на основании заявления Генерального прокурора Российской Федерации или подчиненного ему соответствующего прокурора.

По указанным в части второй настоящей статьи основаниям общественное или религиозное объединение может быть ликвидировано, а деятельность общественного или религиозного объединения, не являющегося юридическим лицом, может быть запрещена по решению суда также на основании заявления федерального органа государственной регистрации или его соответствующего территориального органа. (В редакции Федерального закона от 29.04.2008 г. №54-ФЗ).

В случае принятия судом по основаниям, предусмотренным настоящим Федеральным законом, решения о ликвидации общественного или религиозного объединения их региональные и другие структурные подразделения также подлежат ликвидации.

Оставшееся после удовлетворения требований кредиторов имущество общественного или религиозного объединения либо иной организации, ликвидируемых по основаниям, предусмотренным настоящим Федеральным законом, подлежит обращению в собственность Российской Федерации. Решение об обращении указанного имущества в собственность Российской Федерации выносится судом одновременно с решением о ликвидации общественного или религиозного объединения либо иной организации.

Перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным настоящим Федеральным законом, и описание символики указанных объединений, организаций подлежат размещению в информационно-телекоммуникационной сети «Интернет» на сайтах федеральных органов исполнительной власти, осуществляющих функции в сфере регистрации общественных и религиозных объединений, иных организаций. Указанный перечень также подлежит опубликованию в официальных периодических изданиях, определенных Правительством Российской Федерации. (Часть дополнена – Федеральный закон от 24.07.2007 г. №211-ФЗ) (В редакции федеральных законов от 28.06.2014 г. №179-ФЗ; от 21.07.2014 г. №236-ФЗ).

Статья 10. Приостановление деятельности общественного или религиозного объединения

В случае осуществления общественным или религиозным объединением экстремистской деятельности, повлекшей за собой нарушение прав и свобод человека и гражданина, причинение вреда личности, здоровью граждан, окружающей среде, общественному порядку, общественной безопасности, собственности, законным экономическим интересам физических и (или) юридических лиц, обществу и государству или создающей реальную угрозу причинения такого вреда, соответствующие должностное лицо или орган с момента их обращения в суд по основаниям, предусмотренным статьей 9 настоящего Федерального закона, с заявлением о ликвидации общественного или религиозного объ-

единения либо запрете его деятельности вправе своим решением приостановить деятельность общественного или религиозного объединения до рассмотрения судом указанного заявления.

Решение о приостановлении деятельности общественного или религиозного объединения до рассмотрения судом заявления о его ликвидации либо запрете его деятельности может быть обжаловано в суд в установленном порядке.

В случае приостановления деятельности общественного или религиозного объединения приостанавливаются права общественного или религиозного объединения, его региональных и других структурных подразделений как учредителей средств массовой информации, им запрещается пользоваться государственными и муниципальными средствами массовой информации, организовывать и проводить собрания, митинги, демонстрации, шествия, пикетирование и иные массовые акции или публичные мероприятия, принимать участие в выборах и референдумах, использовать банковские вклады, за исключением их использования для осуществления расчетов, связанных с их хозяйственной деятельностью, возмещением причиненных их действиями убытков (ущерба), уплатой налогов, сборов или штрафов, и расчетов по трудовым договорам.

Если суд не удовлетворит заявление о ликвидации общественного или религиозного объединения либо запрете его деятельности, данное объединение возобновляет свою деятельность после вступления решения суда в законную силу.

Приостановление деятельности политических партий осуществляется в порядке, предусмотренном Федеральным законом «О политических партиях».

Перечень общественных и религиозных объединений, деятельность которых приостановлена в связи с осуществлением ими экстремистской деятельности, подлежит размещению в информационно-телекоммуникационной сети «Интернет» на сайте федерального органа исполнительной власти, осуществляющего функции в сфере регистрации общественных и религиозных объединений. Указанный перечень также подлежит опубликованию в официальных периодических изданиях, определенных Правительством Российской Федерации. (Часть дополнена – Федераль-

ный закон от 24.07.2007 г. №211-ФЗ) (В редакции Федерального закона от 28.06.2014 г. №179-ФЗ).

Статья 11. Ответственность средств массовой информации за распространение экстремистских материалов и осуществление экстремистской деятельности

В Российской Федерации запрещаются распространение через средства массовой информации экстремистских материалов и осуществление ими экстремистской деятельности.

В случае, предусмотренном частью третьей статьи 8 настоящего Федерального закона, либо в случае осуществления средством массовой информации экстремистской деятельности, повлекшей за собой нарушение прав и свобод человека и гражданина, причинение вреда личности, здоровью граждан, окружающей среде, общественному порядку, общественной безопасности, собственности, законным экономическим интересам физических и (или) юридических лиц, обществу и государству или создающей реальную угрозу причинения такого вреда, деятельность соответствующего средства массовой информации может быть прекращена по решению суда на основании заявления уполномоченного государственного органа, осуществившего регистрацию данного средства массовой информации, либо федерального органа исполнительной власти в сфере печати, телерадиовещания и средств массовых коммуникаций, либо Генерального прокурора Российской Федерации или подчиненного ему соответствующего прокурора.

В целях недопущения продолжения распространения экстремистских материалов суд может приостановить реализацию соответствующих номера периодического издания либо тиража аудио- или видеозаписи программы либо выпуск соответствующей теле-, радио- или видеопрограммы в порядке, предусмотренном для принятия мер по обеспечению иска.

Решение суда является основанием для изъятия нереализованной части тиража продукции средства массовой информации, содержащей материал экстремистской направленности, из мест хранения, оптовой и розничной торговли.

Статья 12. Недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности

Запрещается использование сетей связи общего пользования для осуществления экстремистской деятельности.

В случае если сеть связи общего пользования используется для осуществления экстремистской деятельности, применяются меры, предусмотренные настоящим Федеральным законом, с учетом особенностей отношений, регулируемых законодательством Российской Федерации в области связи.

Статья 13. Ответственность за распространение экстремистских материалов

На территории Российской Федерации запрещается распространение экстремистских материалов, а также их производство или хранение в целях распространения. В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность.

Информационные материалы признаются экстремистскими федеральным судом по месту их обнаружения, распространения или нахождения организации, осуществившей производство таких материалов, на основании заявления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому, административному или уголовному делу. (В редакции Федерального закона от 08.03.2015 г. №23-ФЗ).

Одновременно с решением о признании информационных материалов экстремистскими судом принимается решение об их конфискации.

Копия вступившего в законную силу решения о признании информационных материалов экстремистскими направляется судом в трехдневный срок в федеральный орган государственной регистрации.

Федеральный орган государственной регистрации на основании решения суда о признании информационных материалов экстремистскими в течение тридцати дней вносит их в федеральный список экстремистских материалов.

Порядок ведения федерального списка экстремистских материалов устанавливается федеральным органом государственной регистрации.

Федеральный список экстремистских материалов подлежит размещению в информационно-телекоммуникационной сети «Интернет» на официальном сайте федерального органа государственной регистрации.

Указанный список также подлежит опубликованию в средствах массовой информации в установленном порядке. (Статья в редакции Федерального закона от 28.06.2014 г. №179-ФЗ).

Статья 14. Ответственность должностных лиц, государственных и муниципальных служащих за осуществление ими экстремистской деятельности

Высказывания должностного лица, а также иного лица, состоящего на государственной или муниципальной службе, о необходимости, допустимости, возможности или желательности осуществления экстремистской деятельности, сделанные публично, либо при исполнении должностных обязанностей, либо с указанием занимаемой должности, а равно непринятие должностным лицом в соответствии с его компетенцией мер по пресечению экстремистской деятельности влечет за собой установленную законодательством Российской Федерации ответственность.

Соответствующие государственные органы и вышестоящие должностные лица обязаны незамедлительно принять необходимые меры по привлечению к ответственности лиц, допустивших действия, указанные в части первой настоящей статьи.

Статья 15. Ответственность граждан Российской Федерации, иностранных граждан и лиц без гражданства за осуществление экстремистской деятельности

За осуществление экстремистской деятельности граждане Российской Федерации, иностранные граждане и лица без гражданства несут уголовную, административную и гражданско-правовую ответственность в установленном законодательством Российской Федерации порядке.

В целях обеспечения государственной и общественной безопасности по основаниям и в порядке, которые предусмотрены федеральным законом, лицу, участвовавшему в осуществлении экстремистской деятельности, по решению суда может быть ограничен доступ к государственной и муниципальной службе, военной службе по контракту и службе в правоохранительных органах, а также к работе в образовательных организациях и занятию частной детективной и охранной деятельностью. (В редакции Федерального закона от 02.07.2013 г. №185-ФЗ).

В случае если руководитель или член руководящего органа общественного или религиозного объединения либо иной организации делает публичное заявление, призывающее к осуществлению экстремистской деятельности, без указания на то, что это его личное мнение, а равно в случае вступления в законную силу в отношении такого лица приговора суда за преступление экстремистской направленности соответствующие общественное или религиозное объединение либо иная организация обязаны в течение пяти дней со дня, когда указанное заявление было сделано, публично заявить о своем несогласии с высказываниями или действиями такого лица. Если соответствующие общественное или религиозное объединение либо иная организация такого публичного заявления не сделает, это может рассматриваться как факт, свидетельствующий о наличии в их деятельности признаков экстремизма.

Автор печатных, аудио-, аудиовизуальных и иных материалов (произведений), предназначенных для публичного использования и содержащих хотя бы один из признаков, предусмотренных статьей 1 настоящего Федерального закона, признается лицом, осуществлявшим экстремистскую деятельность, и несет ответственность в установленном законодательством Российской Федерации порядке. (Часть дополнена – Федеральный закон от 27.07.2006 г. №148-ФЗ).

Лицо, которое ранее являлось руководителем или членом руководящего органа общественного или религиозного объединения либо иной организации, в отношении которых по основаниям, предусмотренным настоящим Федеральным законом либо Федеральным законом от 6 марта 2006 года №35-ФЗ «О проти-

водействии терроризму», судом принято вступившее в законную силу решение о ликвидации или запрете деятельности, в случаях, предусмотренных законодательством Российской Федерации, не может быть учредителем общественного или религиозного объединения либо иной некоммерческой организации в течение десяти лет со дня вступления в законную силу соответствующего решения суда. (Часть дополнена – Федеральный закон от 31.12.2014 г. №505-ФЗ).

Статья 16. Недопущение осуществления экстремистской деятельности при проведении массовых акций

При проведении собраний, митингов, демонстраций, шествий и пикетирования не допускается осуществление экстремистской деятельности. Организаторы массовых акций несут ответственность за соблюдение установленных законодательством Российской Федерации требований, касающихся порядка проведения массовых акций, недопущения осуществления экстремистской деятельности, а также ее своевременного пресечения. Об указанной ответственности организаторы массовой акции до ее проведения предупреждаются в письменной форме органами внутренних дел Российской Федерации.

Участникам массовых акций запрещается иметь при себе оружие (за исключением тех местностей, где ношение холодного оружия является принадлежностью национального костюма), а также предметы, специально изготовленные или приспособленные для причинения вреда здоровью граждан или материального ущерба физическим и юридическим лицам.

При проведении массовых акций не допускаются привлечение для участия в них экстремистских организаций, использование их символики или атрибутики, а также распространение экстремистских материалов.

В случае обнаружения обстоятельств, предусмотренных частью третьей настоящей статьи, организаторы массовой акции или иные лица, ответственные за ее проведение, обязаны незамедлительно принять меры по устранению указанных нарушений. Несоблюдение данной обязанности влечет за собой прекращение массовой акции по требованию представителей органов

внутренних дел Российской Федерации и ответственность ее организаторов по основаниям и в порядке, которые предусмотрены законодательством Российской Федерации.

Статья 17. Международное сотрудничество в области борьбы с экстремизмом

На территории Российской Федерации запрещается деятельность общественных и религиозных объединений, иных некоммерческих организаций иностранных государств и их структурных подразделений, деятельность которых признана экстремистской в соответствии с международно-правовыми актами и федеральным законодательством.

Запрет деятельности иностранной некоммерческой неправительственной организации влечет за собой:

а) аннулирование государственной аккредитации и регистрации в порядке, установленном законодательством Российской Федерации;

б) запрет пребывания на территории Российской Федерации иностранных граждан и лиц без гражданства в качестве представителей данной организации;

в) запрет на ведение любой хозяйственной и иной деятельности на территории Российской Федерации;

г) запрет публикации в средствах массовой информации любых материалов от имени запрещенной организации;

д) запрет распространения на территории Российской Федерации материалов запрещенной организации, а равно иной информационной продукции, содержащей материалы данной организации;

е) запрет на проведение любых массовых акций и публичных мероприятий, а равно участие в массовых акциях и публичных мероприятиях в качестве представителя запрещенной организации (или ее официальных представителей);

ж) запрет на создание ее организаций-правопреемников в любой организационно-правовой форме.

После вступления в силу решения суда о запрете деятельности иностранной некоммерческой неправительственной организации уполномоченный государственный орган Российской Федерации

обязан в десятидневный срок уведомить дипломатическое представительство или консульское учреждение соответствующего иностранного государства в Российской Федерации о запрете деятельности на территории Российской Федерации данной организации, причинах запрета, а также о последствиях, связанных с запретом.

Российская Федерация в соответствии с международными договорами Российской Федерации сотрудничает в области борьбы с экстремизмом с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями, осуществляющими борьбу с экстремизмом.

Президент Российской Федерации В. Путин

Москва, Кремль
25 июля 2002 года
№114-ФЗ

Приложение 3

Указ Президента РФ от 29 мая 2020 г. №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года»

1 июня 2020

В целях обеспечения дальнейшей реализации государственной политики в сфере противодействия экстремизму в Российской Федерации постановляю:

1. Утвердить прилагаемую новую редакцию Стратегии противодействия экстремизму в Российской Федерации до 2025 года.

2. Настоящий Указ вступает в силу со дня его подписания.

Президент Российской Федерации В. Путин
Москва, Кремль
29 мая 2020 года
№344

УТВЕРЖДЕНА
Указом Президента Российской Федерации
от 29 мая 2020 г. №344

Стратегия противодействия экстремизму в Российской Федерации до 2025 года

I. Общие положения

1. Настоящая Стратегия разработана в целях обеспечения дальнейшей реализации государственной политики в сфере противодействия экстремизму в Российской Федерации, а также в целях конкретизации положений Федерального закона от 25 июля 2002 г. №114-ФЗ «О противодействии экстремистской деятельности» и Указа Президента Российской Федерации от 31 декабря 2015 г. №683 «О Стратегии национальной безопасности Российской Федерации». Одним из основных источников угроз национальной безопасности Российской Федерации является экстремистская деятельность, осуществляемая националистически-

ми, радикальными общественными, религиозными, этническими и иными организациями и объединениями, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной обстановки в стране.

2. Настоящая Стратегия является документом стратегического планирования, который определяет цель, задачи и основные направления государственной политики в сфере противодействия экстремизму с учетом стоящих перед Российской Федерацией вызовов и угроз и направлен на консолидацию усилий федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, институтов гражданского общества, организаций и граждан в целях обеспечения национальной безопасности Российской Федерации, пресечения экстремистской деятельности, укрепления гражданского единства, достижения межнационального (межэтнического) и межконфессионального согласия, сохранения этнокультурного многообразия народов Российской Федерации, формирования в обществе атмосферы нетерпимости к экстремистской деятельности и распространению экстремистских идей.

3. Правовую основу настоящей Стратегии составляют Конституция Российской Федерации, федеральные конституционные законы, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

4. Для целей настоящей Стратегии используются следующие основные понятия:

а) идеология насилия – совокупность взглядов и идей, оправдывающих применение насилия для достижения политических, идеологических, религиозных и иных целей;

б) радикализм – бескомпромиссная приверженность идеологии насилия, характеризующаяся стремлением к решительному и кардинальному изменению основ конституционного строя Российской Федерации, нарушению единства и территориальной целостности Российской Федерации;

в) экстремистская идеология – совокупность взглядов и идей, представляющих насильственные и иные противоправные дей-

ствия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов;

г) проявления экстремизма (экстремистские проявления) – общественно опасные противоправные действия, совершаемые по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, способствующие возникновению или обострению межнациональных (межэтнических), межконфессиональных и региональных конфликтов, а также угрожающие конституционному строю Российской Федерации, нарушению единства и территориальной целостности Российской Федерации;

д) субъекты противодействия экстремизму – федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления;

е) противодействие экстремизму – деятельность субъектов противодействия экстремизму, направленная на выявление и устранение причин экстремистских проявлений, а также на предупреждение, пресечение, раскрытие и расследование преступлений экстремистской направленности, минимизацию и (или) ликвидацию их последствий.

II. Основные источники угроз экстремизма в современной России

5. Экстремизм во всех его проявлениях ведет к нарушению гражданского мира и согласия, основных прав и свобод человека и гражданина, подрывает государственную и общественную безопасность, создает реальную угрозу суверенитету, единству и территориальной целостности Российской Федерации, сохранению основ конституционного строя Российской Федерации, а также межнациональному (межэтническому) и межконфессиональному единению, политической и социальной стабильности.

6. Экстремизм является одной из наиболее сложных проблем современного российского общества, что связано в первую очередь с многообразием его проявлений, неоднородным составом экстремистских организаций, деятельность которых угрожает национальной безопасности Российской Федерации.

7. На современном этапе отмечается тенденция к дальнейшему распространению радикализма среди отдельных групп населения и обострению внешних и внутренних экстремистских угроз.

8. Внешними экстремистскими угрозами являются поддержка и стимулирование рядом государств деструктивной деятельности, осуществляемой иностранными или международными неправительственными организациями, направленной на дестабилизацию общественно-политической и социально-экономической обстановки в Российской Федерации, нарушение единства и территориальной целостности Российской Федерации, включая инспирирование «цветных революций», на разрушение традиционных российских духовно-нравственных ценностей, а также содействие деятельности международных экстремистских и террористических организаций, в частности распространению экстремистской идеологии и радикализма в обществе.

9. Внутренними экстремистскими угрозами являются попытки осуществления националистическими, радикальными общественными, религиозными, этническими и иными организациями и объединениями, отдельными лицами экстремистской деятельности для реализации своих целей, распространение идеологии насилия, склонение, вербовка или иное вовлечение российских граждан и находящихся на территории страны иностранных граждан в деятельность экстремистских сообществ и иную противоправную деятельность, а также формирование замкнутых этнических и религиозных анклавов.

К внутренним угрозам также относятся межнациональные (межэтнические) и территориальные противоречия и конфликты в отдельных субъектах Российской Федерации, обусловленные историческими и социально-экономическими особенностями и приводящие к сепаратистским проявлениям, заключающимся в попытках нарушения территориальной целостности Российской Федерации (в том числе отделения части ее территории) или дезинтеграции государства, а также в организации и подготовке таких действий, пособничестве в их совершении, подстрекательстве к их осуществлению.

10. Экстремизм распространяется за пределы отдельных государств и представляет глобальную угрозу безопасности всего мирового сообщества. Некоторыми государствами экстремизм используется в качестве средства для достижения таких геополитических целей, как нарушение территориальной целостности государств – геополитических противников или развязывание в них гражданских войн, а также для инспирирования «цветных революций» в этих государствах.

11. Реальную угрозу представляют участившиеся в иностранных государствах случаи умышленного искажения истории, возрождения идей нацизма и фашизма.

12. Количество преступлений экстремистской направленности достаточно мало по сравнению с общим количеством иных совершаемых на территории Российской Федерации преступлений, однако каждое такое преступление способно вызвать повышенный общественный резонанс и дестабилизировать внутриполитическую и социальную обстановку как в отдельном регионе, так и в стране в целом.

13. Наиболее опасными проявлениями экстремизма являются возбуждение ненависти либо вражды, унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а также принадлежности к какой-либо социальной группе, в том числе путем распространения призывов к насильственным действиям, прежде всего с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»; вовлечение отдельных лиц в деятельность экстремистских организаций; организация и проведение несогласованных публичных мероприятий (включая протестные акции), массовых беспорядков; подготовка и совершение террористических актов.

14. Информационно-телекоммуникационные сети, включая сеть «Интернет», стали основным средством связи для экстремистских организаций, которые используются ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии.

15. В современных социально-политических условиях крайним проявлением экстремизма является терроризм, который основывается на экстремистской идеологии. Угроза терроризма будет сохраняться до тех пор, пока существуют источники и каналы распространения экстремистской идеологии.

16. Экстремистская идеология является основным фактором, объединяющим членов экстремистских организаций, формирующим характер и направленность их деятельности, а также средством вовлечения в экстремистскую деятельность представителей различных слоев населения.

17. Распространение экстремистской идеологии, в частности мнения о приемлемости насильственных действий для достижения поставленных целей, угрожает государственной и общественной безопасности ввиду усиления агрессивности и увеличения масштабов пропаганды экстремистской идеологии в обществе.

18. Одним из основных способов дестабилизации общественно-политической и социально-экономической обстановки в Российской Федерации становится привлечение различных групп населения к участию в несогласованных публичных мероприятиях (включая протестные акции), которые умышленно трансформируются в массовые беспорядки.

19. Участились случаи привлечения в ряды экстремистских организаций несовершеннолетних лиц, поскольку они не только легче поддаются идеологическому и психологическому воздействию, но и при определенных обстоятельствах не подлежат уголовной ответственности. Многие экстремистские организации используют религиозный фактор для привлечения в свои ряды новых членов, разжигания и обострения межнациональных (межэтнических) и межконфессиональных конфликтов, которые создают угрозу территориальной целостности Российской Федерации.

20. Сохраняющиеся очаги терроризма, межнациональной розни, религиозной вражды и иных проявлений экстремизма, прежде всего в регионах Ближнего Востока и Северной Африки, способствуют интенсификации миграционных потоков, с которыми в Российскую Федерацию проникают члены международных экстремистских и террористических организаций, а также распространению и пропаганде экстремистской идеологии, в том

числе в сети «Интернет».

21. Серьезную тревогу вызывает проникновение из других государств лиц, проходивших обучение в теологических центрах и проповедующих исключительность радикальных религиозных течений и насильственные методы их распространения. Отмечаются попытки создания в различных регионах России законспирированных ячеек экстремистских и террористических организаций, в том числе путем дистанционной вербовки людей (с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет») и их обучения, включая подготовку террористов-одиночек. Кроме того, происходит процесс распространения радикальных взглядов среди трудовых мигрантов, прибывающих в Россию, их вовлечение в совершение преступлений экстремистской направленности.

22. Особую опасность представляют приверженцы радикальных течений ислама, в частности не относящиеся к представителям народов, традиционно исповедующих ислам, однако отличающиеся религиозным фанатизмом, вследствие чего их легко склонить к совершению террористических актов, в том числе в качестве смертников.

23. Одним из факторов, способствующих возникновению экстремистских проявлений, является сложившаяся в отдельных субъектах и населенных пунктах Российской Федерации неблагоприятная миграционная ситуация, которая приводит к дестабилизации рынка труда, социально-экономической обстановки, оказывает негативное влияние на межнациональные (межэтнические) и межконфессиональные отношения.

24. Лидеры экстремистских организаций в своей деятельности ориентируются преимущественно на молодежь, при этом повышенное внимание они проявляют к отличающимся высокой степенью организованности неформальным объединениям националистов, активно привлекая их членов в свои ряды, провоцируя на совершение преступлений экстремистской направленности.

25. Сильную тревогу вызывает распространение радикализма в спортивной сфере, в том числе в спортивных школах и клубах, а также проникновение приверженцев экстремистской идеологии в тренерско-преподавательский состав.

26. Специальные службы и организации отдельных государств наращивают информационно-психологическое воздействие на население России, прежде всего на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей, дестабилизации внутриполитической и социальной обстановки.

27. Значительное негативное влияние на ситуацию в стране оказывает деструктивная деятельность некоторых иностранных организаций и подконтрольных им российских объединений, осуществляемая в том числе под видом гуманитарных, образовательных, культурных, национальных и религиозных проектов, включая инспирирование протестной активности населения с использованием социально-экономического, экологического и других факторов.

28. Прямые или косвенные последствия экстремизма затрагивают все основные сферы общественной жизни: политическую, экономическую и социальную. Это выдвигает новые требования к организации деятельности по противодействию экстремизму на всех уровнях, а также по минимизации его последствий.

III. Цель, задачи и основные направления государственной политики в сфере противодействия экстремизму

29. Целью государственной политики в сфере противодействия экстремизму является защита основ конституционного строя Российской Федерации, государственной и общественной безопасности, прав и свобод граждан от экстремистских угроз.

30. Достижение указанной цели должно осуществляться путем реализации на федеральном, региональном и муниципальном уровнях мер организационного и правового характера, разрабатываемых с учетом результатов мониторинга в сфере противодействия экстремизму.

31. Задачами государственной политики в сфере противодействия экстремизму являются:

а) создание единой государственной системы мониторинга в сфере противодействия экстремизму;

б) совершенствование законодательства Российской Федерации и правоприменительной практики в сфере противодействия экстремизму;

в) консолидация усилий субъектов противодействия экстремизму, институтов гражданского общества и иных заинтересованных организаций;

г) организация в средствах массовой информации, информационно-телекоммуникационных сетях, включая сеть «Интернет», информационного сопровождения деятельности субъектов противодействия экстремизму, а также реализация эффективных мер, направленных на информационное противодействие распространению экстремистской идеологии;

д) разработка и осуществление комплекса мер по повышению эффективности профилактики, выявления и пресечения преступлений и административных правонарушений экстремистской направленности.

32. Основными направлениями государственной политики в сфере противодействия экстремизму являются:

а) в области законодательной деятельности:

обеспечение эффективного применения норм законодательства Российской Федерации в сфере противодействия экстремизму;

проведение мониторинга правоприменительной практики в сфере противодействия экстремизму;

совершенствование законодательства Российской Федерации в сфере противодействия экстремизму в части, касающейся пресечения производства и распространения экстремистских материалов, в том числе на электронных носителях информации, а также в информационно-телекоммуникационных сетях, включая сеть «Интернет»;

совершенствование механизмов противодействия деструктивной деятельности иностранных или международных неправительственных организаций;

принятие на региональном и муниципальном уровнях соответствующих целевых программ, предусматривающих формирование системы профилактики экстремизма и терроризма, предупреждения межнациональных (межэтнических) конфликтов;

принятие управленческих решений, разработка проектов нормативных правовых актов и программных документов в сфере противодействия экстремизму с учетом национального, социально-культурного, религиозного и регионального факторов;

б) в области правоохранительной деятельности:

координация деятельности правоохранительных органов, органов государственной власти, органов местного самоуправления в совместной работе с институтами гражданского общества и организациями по выявлению и пресечению экстремистских проявлений, инспирирования «цветных революций», реализуемых с использованием политического, социального, религиозного и национального факторов;

проведение профилактической работы с лицами, подверженными влиянию экстремистской идеологии;

реализация принципа неотвратимости и соразмерности наказания за осуществление экстремистской деятельности;

повышение эффективности работы правоохранительных органов по выявлению и пресечению изготовления, хранения и распространения экстремистских материалов, символики и атрибутики экстремистских организаций;

организация профессиональной подготовки сотрудников правоохранительных органов и получения ими дополнительного профессионального образования по утвержденным в установленном порядке учебным программам в области выявления, пресечения, раскрытия, расследования, профилактики и квалификации экстремистских проявлений;

совершенствование процедуры проведения экспертизы материалов, предположительно содержащих информацию экстремистского характера;

обеспечение совместно с органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организаторами собраний, митингов, демонстраций, шествий и других публичных мероприятий безопасности граждан и общественного порядка в местах их проведения;

обеспечение взаимодействия субъектов противодействия экстремизму на приграничных территориях в целях пресечения проникновения на территорию Российской Федерации членов международных экстремистских и террористических организаций;

выявление и устранение источников и каналов финансирования экстремистской и террористической деятельности;

в) в области государственной национальной политики:

проведение мониторинга межрасовых, межнациональных (межэтнических) и межконфессиональных отношений, социально-политической ситуации в Российской Федерации в целях предотвращения возникновения конфликтов либо их обострения, а также выявления причин и условий экстремистских проявлений и минимизации их последствий, в том числе с использованием государственной информационной системы мониторинга в сфере межнациональных и межконфессиональных отношений и раннего предупреждения конфликтных ситуаций;

реализация мер правового и информационного характера по недопущению использования этнического и религиозного факторов в избирательном процессе и в предвыборных программах;

обеспечение реализации прав граждан на свободу совести и свободу вероисповедания без нанесения ущерба религиозным чувствам верующих и национальной идентичности граждан России;

разработка и реализация с участием институтов гражданского общества региональных и муниципальных программ по профилактике экстремизма и противодействию экстремизму;

проведение социологических исследований по вопросам противодействия экстремизму, а также оценка эффективности деятельности субъектов противодействия экстремизму по профилактике экстремизма;

своевременное реагирование субъектов противодействия экстремизму и институтов гражданского общества на возникновение конфликтных ситуаций и факторов, способствующих этому;

мотивирование граждан к информированию субъектов противодействия экстремизму о ставших им известными фактах подготовки к осуществлению экстремистской деятельности, а также о любых обстоятельствах, которые могут способствовать предупреждению экстремистской деятельности, ликвидации или минимизации ее последствий;

предотвращение любых форм дискриминации по признаку социальной, расовой, национальной, языковой, политической, идеологической или религиозной принадлежности;

формирование в обществе атмосферы неприятия пропаганды

и оправдания экстремистской идеологии, ксенофобии, национальной или религиозной исключительности;

г) в области государственной миграционной политики:

совершенствование государственной миграционной политики Российской Федерации в части, касающейся привлечения иностранных работников к деятельности на территории Российской Федерации и определения потребности государства в иностранной рабочей силе;

обеспечение скоординированной деятельности субъектов противодействия экстремизму, направленной на недопущение формирования неблагоприятной миграционной ситуации в стране;

противодействие незаконной миграции, профилактика, предупреждение, выявление и пресечение нарушений миграционного законодательства Российской Федерации, а также совершенствование мер ответственности за такие нарушения;

развитие программ социальной и культурной адаптации иностранных граждан в Российской Федерации и их интеграции в общество, привлечение к реализации и финансированию этих программ работодателей, получающих квоты на привлечение иностранной рабочей силы;

принятие мер, препятствующих возникновению пространственной сегрегации, формированию этнических анклавов, социальной исключенности отдельных групп граждан;

привлечение институтов гражданского общества к деятельности субъектов противодействия экстремизму при соблюдении принципа невмешательства;

всестороннее освещение мер, принимаемых в сфере реализации государственной миграционной политики Российской Федерации на федеральном, региональном и муниципальном уровнях, информирование граждан о текущей миграционной ситуации, ее влиянии на различные аспекты жизни российского общества, а также противодействие распространению в информационном пространстве вызывающих в обществе ненависть и вражду ложных сведений о миграционных процессах;

развитие информационных систем учета иностранных граждан, пребывание которых на территории Российской Федерации является нежелательным;

д) в области государственной информационной политики:

проведение мониторинга средств массовой информации и информационно-телекоммуникационных сетей, включая сеть «Интернет», в целях пресечения распространения экстремистской идеологии и выявления экстремистских материалов, в том числе содержащих призывы к подготовке и совершению террористических актов;

совершенствование мер по ограничению доступа на территории Российской Федерации к информационным ресурсам в информационно-телекоммуникационных сетях, включая сеть «Интернет», распространяющим экстремистскую идеологию;

создание специализированного информационного банка данных экстремистских материалов;

принятие эффективных мер по недопущению ввоза на территорию Российской Федерации экстремистских материалов, а также их изготовления и распространения внутри страны;

использование возможностей средств массовой информации, а также ресурсов сети «Интернет» в целях сохранения межнационального (межэтнического) и межконфессионального согласия, традиционных российских духовно-нравственных ценностей и приобщения к ним молодежи;

содействие заключению соглашений, направленных на решение задач в сфере противодействия экстремизму и терроризму, между организаторами распространения информации в сети «Интернет» и профильными государственными и негосударственными организациями, в том числе иностранными;

проведение тематических встреч с представителями средств массовой информации и интернет-сообщества в целях противодействия распространению экстремистской идеологии;

подготовка и размещение в средствах массовой информации и в информационно-телекоммуникационных сетях, включая сеть «Интернет», социальной рекламы, направленной на патриотическое воспитание молодежи;

координация мер, направленных на информационное противодействие распространению экстремистской идеологии в сети «Интернет» (в том числе в социальных сетях), а также проведение

на регулярной основе работы по разъяснению сути противоправной деятельности, осуществляемой лидерами экстремистских организаций, с привлечением видных деятелей культуры, науки, авторитетных представителей общественности, информационного сообщества, конфессий и национальных объединений;

информирование граждан о деятельности субъектов противодействия экстремизму;

подготовка и распространение информационных материалов о предупреждении и пресечении экстремистской деятельности, ориентированных на повышение бдительности российских граждан, возникновение у них заинтересованности в противодействии экстремизму;

создание и эффективное использование специализированных информационных систем в целях осуществления правоприменительной практики в сфере противодействия экстремизму;

выявление способов оказания экстремистскими организациями информационно-психологического воздействия на население, а также изучение особенностей восприятия и понимания различными группами людей информации, содержащейся в экстремистских материалах;

е) в области образования и государственной молодежной политики:

включение в региональные и муниципальные программы по развитию образования и воспитанию несовершеннолетних мероприятий по формированию у подрастающего поколения уважительного отношения ко всем национальностям, этносам и религиям;

организация досуга детей, подростков, молодежи, семейного досуга, обеспечение доступности для населения объектов культуры, спорта и отдыха, создание условий для реализации творческого и спортивного потенциала, культурного развития граждан;

осуществление мер государственной поддержки системы воспитания молодежи, основанной на традиционных российских духовно-нравственных ценностях;

проведение в образовательных организациях занятий по воспитанию патриотизма, культуры мирного поведения, межнациональной (межэтнической) и межконфессиональной дружбы, по обучению навыкам бесконфликтного общения, а также умению

отстаивать собственное мнение, противодействовать социально опасному поведению (в том числе вовлечению в экстремистскую деятельность) всеми законными способами;

включение в учебные планы, учебно-методические материалы учебных предметов, направленных на воспитание традиционных российских духовно-нравственных ценностей, культуры межнационального (межэтнического) и межконфессионального общения, формирование у детей и молодежи на всех этапах образовательного процесса общероссийской гражданской идентичности, патриотизма, гражданской ответственности, чувства гордости за историю России;

повышение профессионального уровня педагогических работников, разработка и внедрение новых образовательных стандартов и педагогических методик, направленных на противодействие экстремизму;

обеспечение активного участия коллегиальных органов управления образовательных организаций в профилактике экстремизма среди учащихся и студентов;

проведение мониторинга девиантного поведения молодежи, социологических исследований социальной обстановки в образовательных организациях, а также молодежных субкультур в целях своевременного выявления и недопущения распространения экстремистской идеологии;

повышение престижности образования в российских религиозных образовательных организациях, а также применение мер государственной поддержки системы общественного контроля за выездом российских граждан для обучения в иностранных религиозных образовательных организациях;

включение в федеральный государственный образовательный стандарт по специальности «Журналистика» образовательных программ по информационному освещению мер, принимаемых для противодействия экстремизму;

усиление роли координационных органов при федеральных органах исполнительной власти и органах исполнительной власти субъектов Российской Федерации в деятельности по воспитанию патриотизма и формированию общероссийской гражданской идентичности у молодежи;

взаимодействие субъектов противодействия экстремизму с молодежными общественными объединениями, организациями спортивных болельщиков, группами лиц и гражданами в целях профилактики экстремистских проявлений при проведении массовых мероприятий;

совершенствование мер, направленных на профилактику экстремистских проявлений в образовательных организациях;

проведение мероприятий по своевременному выявлению и пресечению фактов радикализации несовершеннолетних;

ж) в области государственной культурной политики:

формирование в Российской Федерации межконфессионального и внутриконфессионального взаимодействия в целях обеспечения гражданского мира и согласия;

включение в программы подготовки работников культуры учебного предмета, направленного на изучение основ духовно-нравственной культуры народов Российской Федерации;

содействие активному распространению идеи исторического единства народов Российской Федерации;

государственная поддержка производства продукции средств массовой информации и создания художественных произведений, направленных на профилактику экстремистских проявлений;

з) в области международного сотрудничества:

укрепление позиций Российской Федерации в международных организациях, деятельность которых направлена на противодействие экстремизму;

развитие международного, межкультурного и межконфессионального взаимодействия как эффективного средства противодействия распространению экстремистской идеологии;

совершенствование взаимодействия федеральных органов государственной власти с компетентными органами иностранных государств в сфере противодействия экстремизму;

продвижение в двустороннем и многостороннем форматах российских инициатив по вопросам противодействия экстремистской деятельности, в том числе осуществляемой с использованием сети «Интернет»;

заключение с иностранными государствами соглашений, направленных на решение задач в сфере противодействия экстремизму;

налаживание международного сотрудничества в сфере противодействия экстремизму на основе строгого соблюдения основных принципов и норм международного права, в частности принципа суверенного равенства государств;

недопущение использования международного сотрудничества в сфере противодействия экстремизму в качестве инструмента реализации политических и геополитических целей;

укрепление ведущей роли государств и их компетентных органов в противодействии экстремизму и развитии международного сотрудничества в этой сфере;

участие в обмене передовым опытом в сфере противодействия экстремизму, включая разработку совместных международно-правовых документов;

организация взаимодействия компетентных органов государств – членов Шанхайской организации сотрудничества в рамках реализации Конвенции Шанхайской организации сотрудничества по противодействию экстремизму, подписанной Российской Федерацией 9 июня 2017 г., а также принятие мер, направленных на присоединение к данной Конвенции других государств;

и) в области обеспечения участия институтов гражданского общества в реализации государственной политики в сфере противодействия экстремизму:

государственная поддержка институтов гражданского общества (в том числе ветеранских и молодежных организаций), деятельность которых направлена на профилактику экстремистских проявлений, и использование их потенциала в целях патриотического воспитания граждан, обеспечения единства многонационального народа Российской Федерации, формирования в обществе атмосферы нетерпимости к экстремистской деятельности, неприятия экстремистской идеологии и применения насилия для достижения политических, идеологических, религиозных и иных целей;

привлечение социально ориентированных некоммерческих организаций к реализации проектов, направленных на укрепление межнационального (межэтнического) и межконфессионального согласия, сохранение исторической памяти и патриотическое воспитание молодежи, профилактику социально опасного

поведения граждан и содействие духовно-нравственному развитию личности;

участие общественных советов и иных консультативных органов, созданных при государственных органах и органах местного самоуправления, в деятельности по гармонизации межнациональных (межэтнических) и межконфессиональных отношений;

оказание содействия средствам массовой информации в широком и объективном освещении деятельности субъектов противодействия экстремизму.

IV. Инструменты и механизмы реализации настоящей Стратегии

33. Инструментами реализации настоящей Стратегии являются:

а) нормативные правовые акты Российской Федерации в сфере противодействия экстремизму;

б) документы стратегического планирования, разработанные на федеральном, региональном и муниципальном уровнях;

в) государственные программы в сфере противодействия экстремизму.

34. План мероприятий по реализации настоящей Стратегии разрабатывает и утверждает Правительство Российской Федерации.

35. Реализацию настоящей Стратегии осуществляют субъекты противодействия экстремизму в соответствии с их компетенцией, а также институты гражданского общества и иные заинтересованные организации.

36. Механизмами реализации настоящей Стратегии являются:

а) формирование и исполнение расходных обязательств Российской Федерации, субъектов Российской Федерации и муниципальных образований, предусматривающих ресурсное обеспечение мероприятий по противодействию экстремизму;

б) подбор, расстановка, воспитание кадров, способных обеспечить выполнение мероприятий по противодействию экстремизму, в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, органах местного самоуправления;

в) обеспечение принятия законодательных и иных нормативных правовых актов Российской Федерации, субъектов Россий-

ской Федерации и муниципальных правовых актов, направленных на противодействие экстремизму;

г) обеспечение неотвратимости уголовного наказания и административной ответственности за совершение преступлений и административных правонарушений экстремистской направленности;

д) оказание содействия средствам массовой информации в широком и объективном освещении ситуации в сфере противодействия экстремизму;

е) контроль за исполнением норм законодательства Российской Федерации в сфере противодействия экстремизму и выполнением мероприятий, предусмотренных планом реализации настоящей Стратегии, а также планами и программами по противодействию экстремизму, утверждаемыми субъектами противодействия экстремизму;

ж) активное вовлечение в работу по противодействию экстремизму общественных объединений и других институтов гражданского общества.

37. Координацию реализации настоящей Стратегии осуществляет Межведомственная комиссия по противодействию экстремизму в Российской Федерации.

38. Эффективность реализации настоящей Стратегии обеспечивается согласованными действиями субъектов противодействия экстремизму при осуществлении политических, правовых, организационных, информационных и иных мер, разработанных в соответствии с настоящей Стратегией.

39. Информационно-аналитическое обеспечение реализации настоящей Стратегии в субъектах Российской Федерации и муниципальных образованиях осуществляется с использованием информационных ресурсов субъектов противодействия экстремизму, государственных научных и образовательных организаций, региональных средств массовой информации и некоммерческих организаций.

V. Основные этапы реализации настоящей Стратегии

40. Реализация настоящей Стратегии осуществляется в два этапа.

41. На первом этапе реализации настоящей Стратегии планируется осуществить следующие мероприятия:

а) разработка и принятие законодательных и иных нормативных правовых актов Российской Федерации, субъектов Российской Федерации, направленных на противодействие экстремизму;

б) выполнение мероприятий, предусмотренных планом мероприятий по реализации настоящей Стратегии;

в) проведение мониторинга результатов, достигнутых при реализации настоящей Стратегии;

г) прогнозирование развития ситуации в области межнациональных (межэтнических) и межконфессиональных отношений в Российской Федерации и возникновения экстремистских угроз;

д) обеспечение вовлечения институтов гражданского общества в деятельность, направленную на противодействие экстремизму;

е) создание системы дополнительной защиты информационно-телекоммуникационных сетей, включая сеть «Интернет», от проникновения экстремистской идеологии.

42. На втором этапе реализации настоящей Стратегии планируется обобщить результаты ее реализации и при необходимости подготовить предложения по разработке новых документов стратегического планирования в сфере противодействия экстремизму.

VI. Целевые показатели реализации настоящей Стратегии

43. Целевыми показателями реализации настоящей Стратегии являются:

а) динамика изменения количества зарегистрированных преступлений и административных правонарушений экстремистской направленности, выявленных лиц, совершивших такие преступления и правонарушения, по годам;

б) доля преступлений насильственного характера в общем количестве преступлений экстремистской направленности (в процентах) по годам;

в) количество общественных, религиозных объединений и организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 г. №114-ФЗ «О противодействии экстремистской деятельности»;

г) количество содержащих экстремистские материалы информационных ресурсов в информационно-телекоммуникационных сетях, включая сеть «Интернет», доступ к которым был ограничен на территории Российской Федерации или с которых такие материалы были удалены.

44. Перечень целевых показателей реализации настоящей Стратегии может уточняться по результатам мониторинга ее реализации.

VII. Ожидаемые результаты реализации настоящей Стратегии

45. Ожидаемыми результатами реализации настоящей Стратегии являются:

а) сокращение количества экстремистских угроз в Российской Федерации;

б) уменьшение доли преступлений насильственного характера в общем количестве преступлений экстремистской направленности;

в) недопущение распространения экстремистских материалов в средствах массовой информации и сети «Интернет»;

г) повышение уровня взаимодействия субъектов противодействия экстремизму;

д) активное участие институтов гражданского общества в профилактике и предупреждении экстремистских проявлений;

е) формирование в обществе, особенно среди молодежи, атмосферы нетерпимости к экстремистской деятельности, неприятия экстремистской идеологии;

ж) повышение уровня защищенности граждан и общества от экстремистских проявлений.

46. Реализация настоящей Стратегии должна способствовать стабилизации общественно-политической ситуации в стране, сокращению случаев проявления ксенофобии и радикализма в обществе, повышению уровня общественной безопасности, укреплению межнациональных (межэтнических) и межконфессиональных отношений, развитию духовного и гражданского единства многонационального народа Российской Федерации.

Научное издание

Койбаев Борис Георгиевич
Золоева Зарина Тамерлановна

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИСТСКИМ ПРОЯВЛЕНИЯМ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

Корректор — *И.Г. Дзуцева*
Технический редактор — *Е.Н. Маслов*
Компьютерная верстка — *С.А. Булацева*
Дизайн обложки — *Е.Н. Макарова*

Подписано в печать 16.12.2021.
Формат бумаги 60×84 $^{1}/_{16}$. Бум. офс. Печать цифровая.
Гарнитура шрифта «Times New Roman». Усл. п.л. 11,2.
Тираж 300 экз. Заказ №148.

Отпечатано в Издательско-полиграфическом центре ИП Цопановой А.Ю.
362000, г. Владикавказ, пер. Павловский, 3