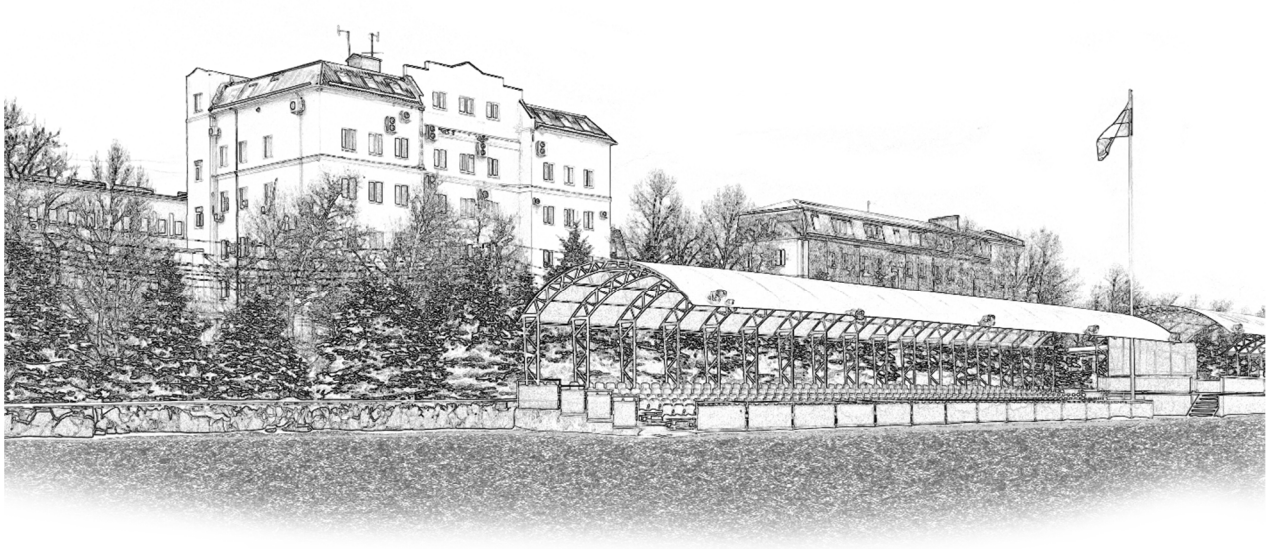
Краснодарский университет МВД России

А. А. Битов
М. Н. Магомедов

МЕТОДЫ И ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ



Краснодар
2025

Краснодарский университет МВД России

А. А. Битов
М. Н. Магомедов

МЕТОДЫ И ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Методические рекомендации

Краснодар
2025

УДК 343.34
ББК 67.515
Б663

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
А. И. Воскобоев, кандидат педагогических наук (Ростовский юридический институт МВД России);
А. З. Ашхотов (МО МВД России «Прохладненский»).

Битов А. А.

Б663 Методы и технологии противодействия проявлениям экстремизма в сети Интернет : методические рекомендации / А. А. Битов, М. Н. Магомедов. – Краснодар : Краснодарский университет МВД России, 2025. – 62 с.

ISBN 978-5-9266-2218-5

Рассматриваются проблемы противодействия экстремистским проявлениям в сети Интернет. Раскрываются способы использования возможностей глобального информационного пространства экстремистскими организациями, а также методы и технологии противодействия им в сети Интернет.

Для профессорско-преподавательского состава, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.34
ББК 67.515

ISBN 978-5-9266-2218-5

Введение

Динамично развивающееся информационное общество на базе информационно-телекоммуникационных технологий относится к общемировым тенденциям современности. Информационное пространство предоставляет широкие возможности, такие как общедоступность, высокая скорость передачи информации, независимость от местонахождения, анонимность и многие другие. Данные преимущества, в том числе – трудность в осуществлении контроля со стороны органов правопорядка, привлекают внимание и криминальных структур, и они активно используют это в своей преступной деятельности, что позволяет им стать менее уязвимыми для правоохранительных органов. Построение современных экстремистских групп организовано по принципу сетевой структуры, которая обеспечивает функционирование единых центров и информационно-коммуникационных каналов. Вместе с этим реализуется автономный способ деятельности периферийных преступных группировок, входящих в сообщество, которые имеют возможность взаимодействовать как с центром, так и друг с другом. Экстремисты активно эксплуатируют возможности сети Интернет, в том числе, мультимедийность среды, позволяющей интегрировать различные типы информации: текстовую, графическую, аудиовизуальную в целях устрашения и запугивания населения. Экстремистскими идеологами широко используются средства психологической

войны, включающие такие, как дезинформация, подмена понятий и фактов, манипуляция общественным сознанием. С момента начала специальной военной операции на Украине вышеуказанные деструктивные явления приняли наиболее масштабный облик с точки зрения ученых и экспертов. Современные информационно-коммуникационные возможности глобальной сети позволяют виртуализированным экстремистским решениям беспрепятственно и бесконтрольно проникать в каждый дом. Наиболее подвержена деструктивному влиянию молодежная среда. Это объясняется свойственными ей социальными характеристиками, в силу которых легче формируются радикальные взгляды и убеждения. В результате молодые люди вовлекаются в преступную деятельность экстремистских и террористических организаций, использующих российскую молодежь в своих интересах.

Сегодня проявления экстремизма и терроризма в глобальном информационном пространстве представляют угрозу безопасности многих стран и их граждан, затрагивают всё человечество и деструктивно влияют на всё мировое сообщество. По словам генерального Прокурора Игоря Краснова на выступлении с ежегодным докладом перед Советом Федерации в апреле 2024 года, в России необходимо пересмотреть законодательство в сфере безопасности: уровень террористических и экстремистских угроз все еще высокий – часть из них исходит от украинских радикальных организаций и сторонников их идеологий, причем каждое третье их преступление совершается через сеть Интернет [12].

По итогам проведенного аналитиками анализа наиболее активно были задействованы возможности таких социальных сетей и мессенджеров , как «Telegramm», «WhatsApp», «ВКонтакте», «Одноклассники», «Facebook» и «Instagram» (последние два запрещены в РФ; принадлежит корпорации Meta, которая признана в РФ экстремистской). По итогам мониторинга российских и иностранных социальных платформ, осуществленного правоохранительными органами в сети Интернет, были обнаружены текстовые, фото и видеоматериалы экстремистского

характера. На 3 мая 2024 года, уже насчитывается 50 организаций, признанных Верховным судом Российской Федерации террористическими [13], деятельность которых запрещена на территории России и 108 организаций, признанных в РФ экстремистскими [14]. В связи с этим, Прокуратура РФ проводит непрерывный мониторинг сети Интернет для обнаружения экстремистских сайтов и ограничения доступа к ним.

Стремительно возрастающее год от года количество активных пользователей сети Интернет, численность которых по расчетам аналитиков на начало 2023 года превысила 5 миллиардов человек (64,4% от всего населения планеты) [15], детерминирует необходимость выработки соответствующих мер обеспечения информационной безопасности глобального информационного пространства, в частности, противодействия активизировавшемуся распространению идей экстремизма и терроризма в глобальной сети.

Глава 1. Способы использования возможностей сети Интернет экстремистскими организациями

1.1. Экстремизм: понятие, виды, проявления

Современная Россия, начиная с 1991 года, под влиянием социальных, политических, экономических и иных обстоятельств, столкнулась с такой проблемой, как «экстремизм». Особо остро экстремистские настроения проявляются в молодежной среде. Проявление экстремизма отмечается в различных сферах общественной жизни, в том числе: социальной и религиозной, политической и экономической. Экстремистские идеологи активно используют в своих преступных целях несовершенство законодательной базы, достижения технического прогресса.

Рассмотрим понятие «экстремизм». В переводе с латинского «extremus» означает «предельный», «критический», «крайний», поэтому данное понятие тесно связано с крайностями. Многие толковые словари, в том числе и словарь С.И. Ожегова [16], трактуют указанное понятие как приверженность к крайним взглядам и мерам, то есть рассматривают его односторонне и связывают только с политикой.

Намного шире рассматриваемое понятие трактуется в юридических источниках, причем в современной юридической литературе есть несколько различных концептуальных подходов к определению понятия «экстремизм».

К примеру, в работах В.В Устинова [17] данное понятие рассматривается как «агрессивное поведение личности, которому свойственны нетерпимость к мнению оппонента, тяготение к силовым способам решения проблемы, неприятие прав личности». Аналогичного толкования придерживаются, в том числе Питер Т. Коулман и Андреа Бартоли [18].

Иной концептуальный подход трактует понятие «экстремизм» как действия, за которые предусмотрена ответственность КоАП РФ и УПК РФ. К примеру, ученые Е.П. Сергун и А.Г. Хлебушкин [19] отмечают, что данная противоправная деятельность

противоречит основным принципам конституционного строя РФ или конституционным основам межличностных отношений».

В.В. Бирюков [20] отмечает, «что экстремизм относится к своеобразной идеологии. Ее цель – обосновать правильность и необходимость совершения различных противоправных деяний по мотивам расовой, национальной или ре-лигиозной нетерпимости». Мнение Власова В.И. [21] идентично.

На основе приведенных выше концептуальных подходов к рассматриваемому понятию, можно указать, что одна из характерных черт данного явления – наличие целей и мотивов по признакам расы, религии, национальности, этносу и т.д., а в качестве объекта преступления (административного правонарушения) могут выступать – государственный строй, государственное управление, а также гражданин (его права и свободы, общественная безопасность).

Ниже рассмотрим законодательное определение данного термина.

В Федеральном законе «О противодействии экстремистской деятельности» [8] понятие «экстремизм» определяется как:

− 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, 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.

К основным видам экстремистской деятельности относятся:

1) Религиозный экстремизм.

Данный вид экстремизма направлен на пропаганду «истинности» одного вероучения и жесткое неприятие идей иных религиозных конфессий, сопровождающееся агрессивным отношением к иноверцам вплоть до их физического уничтожения. Его основной целью является борьба против светского государства либо за провозглашение власти представителей одной из конфессий, пропаганда и распространение своих идей, создание государственных или административных образований, в которых провозглашаемая религия приобрела бы статус официальной и господствующей. Следует отметить, что религиозный экстремизм несет в себе признаки экстремизма политического;

2) Политический экстремизм.

Заключается в незаконной деятельности политических партий и движений, должностных лиц, а также простых граждан. Цель незаконной деятельности – насильственное изменение существующего государственного строя, разрушение существующих государственных структур и установление диктатуры тоталитарного порядка, а также разжигание национальной и социальной нетерпимости и вражды.

3) Националистический экстремизм.

Указанный вид включает в себя элементы как политического, так и религиозного экстремизма.

Высшей формой психологического проявления экстремизма является фанатизм. Он представляет собой крайнюю степень преданности определенной идее и заключается в готовности жертвовать во имя ее не только материальными благами, но и собственной жизнью. Фанатизм является субъективной основой политического экстремизма, выражающееся в слепом, безоговорочном следовании убеждениям, верованиям или воззрениям.

Терроризм относится к глобальной угрозе современности, исследованием которой занимаются многие ученые. Он представляет собой политическое насилие, результат которого – нанесение максимально возможного ущерба, оказание психологического воздействия посредством внушения чувства страха политическим оппонентам. Терроризм является практическим воплощением экс-

тремистского мировоззрения, осуществляемым фанатично настроенными личностями, во имя воплощения радикальных целей, то есть крайней формой проявления политического экстремизма.

Важно отметить, что ряды экстремистских группировок обычно пополняют люди, являющиеся социальными аутсайдерами, которые в силу различных причин не смогли реализоваться в современных условиях. К отмеченной категории относятся, как правило, лица, не имеющие работы; молодые люди, не имеющие образования и достойного уровня жизни. Преступные идеологи для ведения пропаганды, вербовки новых сторонников и увеличения количества «сочувствующих» используют широкомасштабную аудиторию глобальной сети, большую часть пользователей которой составляют молодые люди в возрасте от 12 до 30 лет.

К одной из характерных черт современного экстремизма относится крайняя молодость участников экстремистских группировок. По данным аналитиков, лица в возрасте до 30 лет в среднем составляют около 80 процентов от общего количества участников экстремистских групп [22]. По имеющимся данным сегодня в стране действуют около 150 экстремистских молодежных группировок, в которых состоит около 10 тысяч человек. Большая часть молодых экстремистов проживает в Москве, Санкт-Петербурге, Ростовской, Воронежской и Нижегородской областях.

К наиболее значимым детерминантам молодежного экстремизма относят следующие:

– обострение социальных противоречий в молодежной среде;

– активная пропаганда молодежных националистических группировок экстремистской направленности;

– крушение социальных идеалов молодежи, приведшее к распространению криминальной субкультуры в молодежной среде и вовлечению молодых людей в преступную деятельность;

– усиливающееся влияние «исламского фактора» (пропаганда среди молодых мусульман организаций и движений, в частности структур радикального толка, идей религиозного экстремизма; организация обучения молодежи в странах исламского мира и как следствие – последующая вербовка в международные экстремистские и террористические группировки);

– деформация российской семьи, как основного института социализации, передающего социальные ценности от поколения к поколению и как следствие -неспособность института семьи обеспечить должный уровень социализации среди молодежи;

– использование информационных технологий, развития компьютеризации и информатизации, возможностей Интернет-пространства в целях информационного обеспечения противоправной деятельности радикальных сообществ и групп;

– использование в деструктивных целях психофизиологических особенностей подросткового возраста: агрессии, нетерпимости, максимализма, которые активно используются адептами молодежных группировок экстремистско-националистической направленности для осуществления террористических акций.

Особую актуальность в образовательном учреждении приобретает деятельность по профилактике молодежного экстремизма. Подростку необходима среда, где есть возможность быть принятым таким, каков он есть.

В настоящий момент официально известно о более чем 20 нападениях в учебных заведениях страны. Кроме того, оперативные службы активно занимаются предотвращением подобных актов терроризма до их непосредственного совершения. В целях противодействия вербовке школьников и студентов для нападений в учебных заведениях в 2022 году Росфинмониторинг внёс «Колумбайн» (организация признана в РФ террористической, деятельность запрещена) в список экстремистских организаций, запрещённых на территории РФ. Данная организация вела деятельность и на территории РФ [23].

1.2. Экстремизм в сети Интернет: понятие и особенности проявления

Как было обозначено выше, в современном информационном обществе отмечается развитие такой тенденции, как перемещение экстремизма в глобальное информационное пространство, а именно его переход в информационный экстремизм. С каждым годом это явление набирает обороты и в сегодня уже вышло на мировой уровень.

Глобальная сеть на современном этапе развития общества широко используется как средство массовой коммуникации, можно сказать, что сеть Интернет является мировым хранилищем различной информации.

В «Стратегии противодействия экстремизму в Российской Федерации до 2025 года» отмечено, что информационно-телекоммуникационные сети, включая сеть Интернет, стали основным средством коммуникации для экстремистских и террористических организаций [24]. Радикальные религиозные организации, используя доступ к огромной аудитории глобального информационного пространства, размещают в сети Интернет материалы экстремистского характера, которые оказывают деструктивное информационно-психологическое воздействие на массовое сознание.

Понятие «информационный экстремизм» рассматривалось в работах многих ученых, в том числе Трухачевым В.В., Жуковой О.С., Иванченко Р.Б. В частности, оно трактуется как деятельность, связанная с созданием, хранением и (или) распространением антиобщественной информации, обрабатываемой посредством компьютера, компьютерной системы и (или) компьютерной сети. Согласно законодательным актам данная информация содержит признаки экстремистской деятельности и используется для оказания воздействия на принятие решения органами государственной власти, органами местного самоуправления либо международными организациями. В качестве инструментов воздействия могут использоваться различные методы и средства опосредованного физического или психического насилия, посредством распространения деструктивной информации [25].

Среди основных признаков данного вида экстремизма следует отметить: причинение морального, материального, физического и иного ущерба законным интересам, правам и свободам граждан.

Тактический арсенал информационных экстремистов составляют различные экстремистские методики, направленные на противопоставление религий, народов, убеждений, идеологий, доступ к которым сегодня можно легко получить во всемирной паутине.

Основным оружием информационного экстремизма является повреждение коммуникаций с целью появления хаоса в информационном обществе, а методом – воздействие на огромную по своим масштабам Интернет-аудиторию посредством размещения в сети материалов экстремисткой направленности: аудио-и видеосообщений, документальных фильмов, текстовых материалов, а также ведение пропаганды и агитации посредством личного общения через визуальные средства общения глобальной сети. К таковым относятся многочисленные социальные сервисы, мессенджеры, форумы и микроблоги.

Таким образом, планируемые мероприятия, направленные на профилактику информационного экстремизма должны разрабатываться с учетом изменений в коммуникационных системах современного общества и существенного роста значимости использования сети Интернет.

В настоящее время проблемы обеспечения информационной безопасности в Российской Федерации имеют первостепенное стратегическое значение для обеспечения национальной безопасности страны. При этом система информационной безопасности должна включать следующие три компонента:

– информационно-правовой (наличие соответствующей нормативной базы, определяющей защиту интересов личности, общества и государства в информационной сфере);

– информационно-технический (защита информационной сферы от несанкционированных воздействий);

– информационно-психологический (психологическая безопасность и защита гражданина от негативного информационного воздействия).

В настоящее время ведение информационных войн между странами стало обычным явлением и основной составляющей национальной политики многих государств. Примеров можно привести достаточно много. Это информационные войны, направленные на формирование отрицательного международного общественного мнения посредством ведения массированной дезинформации, которые были развернуты против Ирака, Ливии, Сирии непосредственно перед военным вторжением в эти страны. События, происходящие на Украине, ясно показали, что против России ведётся масштабная агрессивная информационная война, угрожающая национальной безопасности нашей страны.

Очевидно, что в современном мире приоритетное стратегическое значение имеет весьма развитое информационное пространство. Одной из важнейших задач в вопросах обеспечения национальной безопасности является анализ и контроль информационных потоков, цель которого – своевременное выявление и разоблачение агрессивных информационных фантомов.

1.3. Интернет как средство вовлечения пользователей в экстремистские организации

Экстремистские и радикальные сообщества активно используют сеть Интернет в целях вербовки новых сторонников в свои ряды. А.С. Пржездомский – представитель Национального антитеррористического комитета отметил, что «бесконтактные» вербовки во всемирной сети сегодня приобретают глобальный характер [26]. Экстремистские идеологи в кратчайшие сроки формируют психологический портрет собеседника, вступившего в общение с ними на форуме, чате или мессенджере. Затем к потенциальному вербуемому находят индивидуальный подход и устанавливают возможные способы его применения в рамках деятельности экстремистской организации. Таким образом, молодые люди, совершенно даже не замечая этого, оказываются вовлеченными в преступную деятельность. Чаще всего, это лица, не достигшие совершеннолетия, которым в силу их возраста характерен юношеский максимализм, чем часто пользуются экстремистские силы, устремляя подростка в деструктивное русло радикализма.

В трудах Ю. И. Сундиева [27] отмечено, что среди основных задач, которые решаются руководителями экстремистских организаций с помощью использования социальных платформ – деятельность по вербовке новобранцев. Она заключаются в создании на основе информационно-манипулятивных технологий наиболее привлекательного образа своего сайта с целью привлечь пользователей и вызвать у них желание вступить в преступную группу.

Почему именно посредством глобального информационного пространства экстремистские организации проводят пропаганду радикальных идей и организуют так называемый «онлайн-рекрутинг» новобранцев? Как упоминалась выше, причина кроется в широких возможностях киберпространства, которое не ограничено ни пространственными, ни временными, ни организационными и технологическими рамками. У пользователей глобальной сети есть возможность находится на связи круглосуточно, с любых географических точек, сохраняя при этом анонимность.

Поскольку отсутствует прямой контакт между экстремистами и пользователями социальных платформ, преступниками

могут без ограничений использоваться все необходимые инструменты манипулятивной техники, с помощью которой обеспечивается неосознанность действий большинства вовлекаемых, их непонимание своего участия в экстремистской деятельности.

Своих сторонников в социальных сетях активисты преступных организаций называют такими же воинами джихада, как и бойцов сирийских группировок. Все начинается по отработанной схеме, с безобидного бытового общения в чатах социальных сервисов, постепенно оно переходит в обучение по религиозным вопросам, далее подопечные вступают в закрытые группы, имеющие высокий уровень криптозащиты, где уже на завершающем этапе и происходит окончательная вербовка. После этого, с учетом личности завербованного, определяется где и в каких целях можно его использовать.

Завербованный привлекается к определенному виду противоправной деятельности, в том числе:

– идеолого-пропагандистской работе – для ведения которой производится оценка способностей новобранца генерировать новые идеи в русле экстремистских концепций. Отбор и вербовка потенциальных кандидатов производятся на веб-сервисах радикальной направленности, причем экстремистами адептами отбираются наиболее активные участники, которые могут грамотно и понятно излагать свои мысли, отстаивать свою точку зрения, убеждать. После постепенного привлечения новобранца к сотрудничеству, вербовщики используют «интеллектуальный крючок», заключающийся в выполнении кандидатом ряда сложных, но захватывающих интеллектуальных заданий. Решая поставленные задачи, кандидаты проходят проверку на пригодность и одновременно учувствуют в экстремистской деятельности;

– ведению PR-деятельности – заключается в организации и исполнении различного рода информационных акций. К ним относятся владельцы СМИ, в том числе веб-сервисов и журналисты. Этот блок занимается дискредитацией органов государственной власти и давлением на правительственные структуры, в том числе и со стороны международных организаций. Члены данного блока также обеспечивают соответствующее новостное освещение тер-

актов. При этом ими формируется нужный заказчику образ экстремиста, он представляется как «народный мститель», «борец за свободу своего народа» и так далее. За выполнение указанных функций участники данного блока не только получают щедрое вознаграждение, но и возможность выходить с эксклюзивными интервью и репортажами, повышающими их рейтинг;

– участию в одноразовых акциях – данный блок вербуемых делится на 3 подгруппы, в их числе: боевики, снабженцы и массовка.

Первую подгруппу формируют из лиц, способных учувствовать в силовых акциях. В Интернет-сервисах им определяются конкретная задача, вероятная цель, место и время совершения акции. В полном составе группа «боевики» встречается только один раз во время выполнения намеченной акции.

К следующей подгруппе, называемой «снабженцами» – относятся лица, которые обеспечивают проведение акций экстремистского и террористического характера. Их подбор осуществляется из общего массива лиц, разделяющих радикальные идеи, которых впоследствии можно будет использовать в случае необходимости. В созданной базе в случае необходимости, всегда можно найти лицо, которое занимает определенную должность, проживает в нужном месте, имеет необходимые связи или знакомства. «Снабженцы», имеющие требуемые характеристики, обычно привлекаются «втемную», при этом, одних и тех же принято использовать только один раз.

В подгруппу «массовка» отбираются лица, обеспечивающие привлечение внимания и увеличение общественного резонанса и масштабности происходящего при проведении экстремистской акции. Эта группа стала востребованной в связи с распространением так называемых «острых флешмобов», привлекающих значительное число лиц из числа поддерживающих экстремистскую идеологию в целях организации экстремистской акции.

Следующий шаг в осуществлении манипуляции заключается в привлечении внимания и возбуждении интереса к размещенной информации, представляемой, к примеру, в виде высокоскоростного мозаичного видеоряда, собранного из эмоционально шокирующих составляющих. Использование данного приема приводит к

некритическому восприятию аудиторией передаваемых сообщений и позволяет значительно усилить внушающий эффект влияния информации в ущерб ее рациональной оценке. Указанная примитивная, но в то же время действенная методика повсеместно используется крупнейшими радикально-экстремистскими, а также террористическими ресурсами. После того, как контакт с объектом установлен, в целях его закрепления активно применяются специальные коммуникативные способы манипулятивного воздействия, включающего логико-психологические и организационные техники. Это может быть персональное обращение, которое составлено с учетом выявленных на предыдущем этапе психологических особенностей вербуемого. В его начале присутствуют открытый протест и заявления сепаратистского характера, основанные на собственной трактовке произошедших исторических и политических событий, затем приводится уличение правительственных структур в «глобальной лжи» и изложение собственной версии происходящего, дискредитирующей официальную власть и, в заключение – представление информационного пакета, направленного на конкретные противоправные действия против личности и государственных структур для достижения «высшей справедливости».

Помимо непосредственной вербовки на Интернет-ресурсах, радикальные экстремисты осуществляют «онлайн-рекрутинг» молодых людей посредством специально созданной сетевой «игры» «Сломай систему». Ее цель «дискредитация органов государственной власти (внесена в Федеральный список экстремистских материалов Министерства Юстиции России) [7].

На первом этапе «онлайн-игры» вербуемый просто участвует в дискуссии. После вербовочных бесед ему предлагают вступить в группу, затем «игрок» выполняет специально разработанные задания, пропагандирующих насилие. По итогам первого этапа вербуемый обязан подготовить отчетный видеоролик. В следующем уровне вербуемый представляет видеоролик, содержащий издевательские меры воздействия на человека. При этом рекрутам оплачивают каждое выполненное задание. Подготовленные видеоотчеты о преступных действиях «играющие» размещают в разделе

«Новости» на портале Интернет-игры, на котором содержатся инструкции по изготовлению взрывных устройств, рекомендации по конспирации и другая информация.

В целях противодействия манипулятивным и новейшим информационно-коммуникативным технологиям, которые сегодня активно используются экстремистскими организациями и радикальными группировками, государство на современном этапе должно уметь применять эффективные методы ведения контрпропаганды в сети Интернет и действовать не только в режиме реакции на действия экстремистов, но и на опережение.

1.4. Использование сети Интернет и ее технических возможностей для оказания деструктивного воздействия на активных пользователей и критически важных объектов

В современном информационном обществе для общения достаточно иметь только компьютер или смартфон с доступом в сеть Интернет. Этой возможностью и пользуются члены экстремистских организаций.

Для экстремизма в сети Интернет характерно наличие специфических особенностей:

- виртуальный характер экстремистской информации, которая доступна широкому кругу лиц без ограничений;
- анонимность, позволяющая экстремистам свободно действовать в глобальном цифровом пространстве;
- широкие возможности для использования мультимедийных технологий, возможность создания экстремистского контента и легкость его передачи;
- сложность доказательства совершения экстремистских действий в сети по причине того, что информация хранится исключительно на оборудовании экстремиста и у независимого провайдера;
- наличие возможности общения в формате онлайн, которое позволяет быстро обмениваться сведениями, содержащими в том числе и экстремистскую информацию.

Эти особенности определяют необходимость решения следующих задач: определения собственника интернет-контента, в котором были размещены экстремистские материалы; идентификации пользователя, разместившего информацию экстремистского содержания; осуществление мер воздействия на собственника интернет-контента с целью удаления информации экстремистского содержания.

На экстремистских веб-сайтах размещается информация о политических и идеологических целях экстремизма, биографические данные основателей и «героев», данные о наиболее громких акциях, жесткая критика «врагов», обзор текущих новостей.

В целях оказания максимального психологического воздействия на массовое сознание сайты экстремистского характера разрабатываются на высоком профессиональном уровне, включают фото-, аудио- и видеофайлы, что способствует привлечению как можно большего числа сторонников.

По аналитическим данным, большая часть контента экстремистского содержания размещена на серверах, территориально расположенных за пределами Российской Федерации. При этом они легально функционируют в большинстве западных стран. Указанный факт делает невозможным осуществление судебного преследования лиц, размещающих в интернет-пространстве антиобщественную информацию [28]. Однако, даже в случае удаления контента экстремистского характера, через некоторое время его заменяет аналогичный новый. Данная схема все чаще используется экстремистскими организациями.

Экстремисты применяют возможности сети Интернет для ведения полномасштабных информационных войн и в целях информационного обеспечения своей деятельности. При этом экстремистскими идеологами используются различные приемы воздействия на сознание человека: распространение дезинформации, провокационных поддельных видеоматериалов, которые способствуют изменению оценки происходящего. Размещаемые веб-ресурсы по продвижению экстремистской, националистической и террористической идеологий носят агрессивный и наступательный характер. Они продуманы и подготовлены с использованием методов управляемого информационно-психологического воздействия на массовое сознание.

Вместе с созданием и поддержанием собственных Интернет-сайтов экстремистские организации проявляют высокую активность на форумах, в социальных сетях, порталах общего доступа. Сегодня общение в социальных сетях – это самое популярное занятие в Интернет-пространстве, на данный момент аудитория социальных сетей насчитывает 4,76 миллиардов пользователей, что на 3 % больше по сравнению с показателем

прошлого 2023 года [15]. Следует отметить, что мобильные телефоны стали приоритетным устройством для пользователей интернета и социальных сетей, в которых ежедневно они проводят почти 7 часов.

В одной из самых популярных в России социальных платформ «ВКонтакте» были выявлены многочисленные группы, завуалированные под «патриотизм», которые на самом деле, проповедовали политический, религиозный, националистический экстремизм.

В июне 2020 года Роскомнадзором по согласованию с Генпрокуратурурой РФ было принято решение разблокировать социальную платформу «Telegram» после того, как основатели сервиса сообщили о готовности противодействовать терроризму и экстремизму. Отмечается, что еженедельно с месенджера «Telegram» удаляется примерно 1,3 тысячи материалов экстремистского и террористического характера. Террористический акт в концертном зале «Крокус Сити Холле» (Красногорск) произошел 22 марта 2024 года, в результате которого погибли не менее 145 человек и 551 человек получил ранения. Террористов завербовали через Telegram-канал «Голос Хорасана» (запрещенная в России террористическая организация), принадлежащему афганскому крылу «Исламского государства» (запрещенная в России террористическая организация) и работающий на аудиторию в Таджикистане [29].

На видеоресурсе «YouTube» каждый день просматривается около 4 миллиардов видеороликов, в число которых входят и ролики экстремистской и террористической направленности. По заявлению Роскомнадзора, сделанного в апреле 2022 года, видеохостинг «YouTube» не ограничивает распространение информации экстремистского характера, содержащей призывы к противоправным действиям против граждан и военных РФ. На текущий момент по заявлению Роскомнадзора, видеохостинг не удалил более 12 тысяч подобных запрещенных материалов.

Социальные сети, мессенджеры и другие интернет-ресурсы в настоящее время являются самыми эффективными инструментами иформационно-психологического воздействия на

общественное сознание и, в частности, на отдельных личностей. Кроме использования сети Интернет для деструктивного воздействия на пользователей, экстремистскими организациями обширно применяются информационно-технические способы воздействия на различные сферы жизнедеятельности России.

Приоритетными секторами для совершения хакерских атак в 1 квартале 2024 году в мире стали следующие секторы [30]:

− организации из сфер образования и исследований (прирост на 73%);

− организации из сферы здравоохранения (увеличение атак на 69%);

− ИТ сервис-провайдеры (прирост на 65%);

− организации из сферы коммуникаций (прирост на 49%);

− организации из государственной и оборонной сферы (прирост на 47%).

Злоумышленники продолжают внедрять новые инструменты и методы для проведения кибератак, особенно с использованием программ-вымогателей. Проблема применения хакерами программно-математических методов информационного оружия для совершения кибератак сегодня вызывает беспокойство всего мирового сообщества, поскольку заключения аналитиков в этой области подтверждают несомненную уязвимость любого государства, с учетом того, что киберпреступник может угрожать информационным системам и автоматизированным системам управления, расположенным почти в любой точке земного шара.

К средствам программно-математического воздействия относятся:

– логическая бомба (Logic Bomb, ЛБ) – так называемая «программная закладка», которая заранее вносится в информационную систему и запускается при определённых временных или информационных условиях для выполнения вредоносных действий;

– компьютерный вирус (Software Virus, КВ) – вид вредоносного программного обеспечения, с возможностями самокопирования, которое внедряясь в «чужую» электронную среду

сначала распространяется в ней, а затем нарушает работу программно-аппаратных комплексов, в том числе, уничтожает информацию или деформирует, удаляет операционную систему, приводит в негодность структуру размещения данных, блокирует работу пользователей и так далее;

– «троянский конь» (The Trojan Horse, разновидность ЛБ) – программа, которая осуществляет скрытый, несанкционированный доступ к информационным ресурсам с целью получения разведывательных данных;

– средства воздействия на каналы обмена информацией посредством создания помех, введения ложных сведений, искажения содержания информации;

– нейтрализаторы тестовых программ (Testing Software Neutralizer) – предназначены для обеспечения невозможности выявления случайных и специально разработанных недостатков программного обеспечения;

– сознательное внесение хакерами в программное обеспечение различного рода ошибок (Software Holes);

– средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах военного и государственного управления, передачи нужной для воздействующей стороны информации.

Использование злоумышленниками приведенных выше средств программно-математического воздействия способно парализовать функционирование информационной инфраструктуры государства, а также подавить всю систему управления вооруженными силами страны. Поэтому современный «электронный джихад» использует массированное применение информационного оружия для осуществления информационно-технического воздействия, обращённого против информационных сфер государства.

Можно привести примеры специальных вредоносных программ, используемых для совершения атак на промышленные предприятия. По заключениям аналитиков, взломать объекты энергетической инфраструктуры не составит труда при наличии специализированных вредоносных программ, разработанных

«под энергетику». Проведенный анализ комплексной вредоносной программы «Industroyer», предназначенной для атак на электроэнергетические компании, выявил, что она обеспечивает хакерам возможность напрямую управлять выключателями и прерывателями цепи на электрических подстанциях. В состав опасного вредоносного кода входит инструмент для выполнения DoS-атак (denial-of-service — отказ в обслуживании), направленный на устройства релейной защиты, представляющих собой комплекс устройств для быстрого выявления и отделения поврежденных элементов для сохранения нормальной работы системы в целом. Статистику подобных кибератак на энергетические системы, как указано аналитиками, привести невозможно, поскольку операторами атомных электростанций не предаются огласке отраженные кибератаки. При этом специалистами отмечено, что подобные атаки на госструктуры и Интернет-сервисы действительно участились.

Самый большой ущерб от кибератаки был зафиксирован в июне 2017 года от вируса «New Petya», «NotPetya» или «ExPetr», атаковавшего крупные корпоративные сети компаний и госслужб по всему миру. Так же, как и «WannaCry» (вредоносная программа-вымогатель, которая была отнесена к самому массовому вирусу десятилетия) «Petya» и его поздние версии поражали компьютеры на ОС «Microsoft Windows». Вирус затронул компании и госорганы Австралии, Европы, США, России, Индии, Украины, Китая. В числе пострадавших были и российские компании «Роснефть» и «Башнефть», а также международные корпорации: «Maersk», «Saint-Gobain», «Reckitt Benckiser» и другие. По данным аналитиков, проникновение вируса на более защищенные объекты, как правило, происходит по вине сотрудников, которые нарушают правила при обращении с устройствами. В частности, есть факты заражения компьютерных систем через «флэшки» сотрудников, которые копировали данные на рабочие компьютеры и таким образом инфицировали систему. Экспертами отмечается, что экстремисты и террористы могут использовать связи в хакерском сообществе для

совершения атак на объекты жизненно важной инфраструктуры, с целью спровоцировать техногенные аварии и экологические катастрофы.

Бесспорно, в России предпринимаются меры для обеспечения информационной безопасности, однако не стоит недооценивать возможности экстремистских организаций, кибератаки которых направлены на то, чтобы вызвать широкий общественный резонанс. С учетом интересов экстремистов к российским информационным ресурсам и финансовым возможностям, можно прогнозировать дальнейший рост угроз для критически важных объектов Российской Федерации.

Глава 2. Методы и технологии противодействия экстремистским проявлениям в сети Интернет

2.1. Законодательная база в сфере противодействия экстремизму в сети Интернет

Как было отмечено выше, в настоящее время особую угрозу не только личности, но и обществу, и в целом национальной безопасности Российской Федерации, представляет стремительное распространение информационного экстремизма. Экстремистские организации используют широкие возможности киберпространства для продвижения экстремистской и террористической идеологий в массы. В соответствии с Концепцией противодействия терроризму в РФ, распространение террористических и экстремистских материалов, осуществляемых с использованием сети Интернет, является одним из ключевых факторов, способствующих распространению идеологии экстремизма в России. В связи с этим, в настоящее время, одной их приоритетных задач органов государственной власти является разработка и внедрение эффективных технологий, направленных на противодействие проявлениям экстремизма в сети Интернет.

Среди основных методов противодействия экстремизму в сети Интернет можно отнести следующие:

– правовые, связанные с совершенствованием нормативно-правовой базы в области противодействия распространению экстремизма, пресечения деятельности экстремистских организаций в сети Интернет;

– информационно-пропагандистские, направленные на активизацию противодействия распространению идеологии экстремизма и терроризма в киберпространстве, использование веб-каналов информации в целях предупреждения и противодействия экстремистской и террористической деятельности;

– технико-технологические методы, которые состоят из систем мониторинга и программ обеспечения информационной безопасности;

– международное сотрудничество в сфере борьбы с проявлениями экстремизма и терроризма в киберпространстве.

Правовые основы доступа к информации в РФ регулируют в первую очередь федеральные законы «Об информации, информационных технологиях и защите информации» и «Об архивном деле в РФ» [4,10]. В соответствии с указанными федеральными законами информация делится на общедоступную и информацию ограниченного доступа. В свою очередь, информация ограниченного доступа делится на сведения, отнесенные к различным видам тайн, в том числе: государственной, коммерческой, служебной, личной и иным видам.

В зависимости от порядка ее предоставления или распространения информация подразделяется на:

1) свободно распространяемую;

2) предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) подлежащую предоставлению или распространению в соответствии с федеральными законами;

4) информацию, распространение которой в РФ ограничено или запрещено.

Глобальное информационное пространство, благодаря широкой распространенности и всеобщей доступности, безусловно, является очень удобным и эффективным источником информации. Вследствие этого использование безграничных возможностей обмена общедоступной информацией во всемирной сети не вызывает никаких споров и сомнений. Однако, в киберпространстве также осуществляется размещение информации, доступ к которой запрещен в целях обеспечения общественной и государственной безопасности. К примеру, сведения о методах разработки, производства и использования наркотических средств; информация о способах совершения самоубийства, а также интернет-ресурсы, содержащие материалы экстремистского и террористического толка. Современный информационный экстремизм ставит под угрозу безопасность общества, нарушая законные права человека, чиня препятствия достижению гражданского согласия, подрывая устои демократического и правового государства. Все это опреде-

ляет борьбу с информационным экстремизмом сегодня как первоочередную задачу особой важности, стоящую перед органами государственной власти.

Одним из первых правовых актов, регламентирующих противодействие экстремизму и терроризму, был Указ Президента РФ 23.03.1995 № 310 «О мерах по обеспечению согласованных действий органов государственной власти в борьбе с проявлениями фашизма и иных форм политического экстремизма в Российской Федерации». В резолютивной части данного нормативного акта было дано указание о необходимости разъяснения понятий и терминов, содержащихся в действующем законодательстве, которыми определяется ответственность за противоправные деяния, приводящие к возбуждению национальной, расовой, религиозной и социальной розни; Министерству внутренних дел совместно с Министерством юстиции России подготовить и представить проекты законов, устанавливающих ответственность за проявления фашизма, а также других форм экстремизма для внесения поправок в уголовное и административное законодательство.

Современная нормативно-правовая база РФ в области противодействия терроризму и экстремизму в глобальной сети базируется на следующих положениях Конституции РФ [1]:

п.5, ст.13 (запрет на создание и функционирование объединений, деятельность которых направлена на разжигание социальной, расовой, национальной и религиозной розни);

п.2 ст.29 (запрет на пропаганду или агитацию, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду).

К основным нормативным актам в сфере противодействия экстремизму и терроризму в РФ, относятся:

– Федеральный закон РФ от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности»;

– Федеральный закон РФ от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;

– «Стратегия противодействия экстремизму в Российской Федерации до 2025 года» от 28 ноября 2014 г. № Пр-2753 (ред. от 29.05.2020);

– «Концепция противодействия терроризму в Российской Федерации» от 5 октября 2009 года.

По статистическим данным правоприменительной практики можно выделить нормы, которые чаще всего используются судебными органами в связи с реализацией в сети Интернет пропаганды идей экстремизма и терроризма.

К ним, в том числе, относят:

– нормы Уголовного кодекса Российской Федерации (ч. 2 ст. 280, ст. 281, ст. 282, 282.1, 282.2, 282.3);

– нормы Кодекса Российской Федерации об административных правонарушениях (ст. 20.3, 20.3.1, 20.3.2, 20.29).

Следует отметить, что применение статьи 282 УК РФ вызвало множество нареканий и споров в юридическом сообществе. Размытость формулировки с одной стороны и сложность доказывания наличия прямого умысла в разжигании ненависти с другой, делают указанную норму малоэффективной, с точки зрения защиты основ конституционного строя и более того представляет угрозу социальной стабильности. По статистике Генпрокуратуры, большую часть уголовных дел по статье 282 УК РФ возбуждали именно за публикации в сети Интернет. При этом за репосты в социальных сетях материалов, которые были признаны экстремистскими, граждан осуждали на реальные тюремные сроки. Число осужденных по указанной норме непрерывно увеличивалось. К примеру, если в 2015 году по статье 282 УК РФ было осуждено 444 человека, то в 2016 году – 502 человека, а в 2017 году число осужденных выросло до 571 человека [31].

Практика правоприменения данной нормы обозначила необходимость внесения соответствующих корректив. Пакет поправок, касающийся частичной декриминализации статьи 282 УК РФ, был внесен в Госдуму Президентом России Владимиром Путиным 3 октября 2018 года. Цель поправок – недопущение случаев привлечения к уголовной ответственности за деяния, которые были совершены однократно и не представляли серьезную угрозу основам конституционного строя и безопасности государства. В данном случае совершенные действия повлекут административную ответственность. Однако если в течение года правонарушение бу-

дет совершено повторно, будет применяться уголовная ответственность в соответствии со статьей 282 УК РФ. Предлагаемые Президентом РФ поправки позволят отделить настоящих экстремистов от тех, кто по незнанию распространил экстремистский материал, делая, в частности, репосты сообщений.

В 2016 году был принят так называемый антитеррористический «пакет Яровой», направленный на предотвращение развития экстремистских организаций. Пакет включает два федеральных закона: № 374-ФЗ [6], и № 375-ФЗ [11].

Поправки, внесенные пакетом в Федеральное законодательство, состоят из следующих компонентов:

– разработка и внедрение новых требований к Интернет-провайдерам и операторам связи;

– расширение полномочий правоохранительных органов;

– разработка и внедрение новых требований к перевозчикам-экспедиторам и почтовой связи;

На основании федерального закона №374-ФЗ внесены поправки в статью 10.1 федерального закона №149-ФЗ «Об информации, информационных технологиях и о защите информации» в том числе пункт 3 изложен в следующей редакции:

«Организатор распространения информации в сети Интернет обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством РФ.

Организатор распространения информации в сети Интернет обязан предоставлять указанную в пункте 3 информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности

Российской Федерации, в случаях, установленных федеральными законами».

«Закон Яровой» вызвал массу обсуждений. В связи с принятием данного закона многие специалисты высказывали мнение о возникновении существенных сложностей при дальнейшем оказании услуг в своей сфере. С самыми значительными затруднениями на сегодняшний день столкнулись мобильные операторы, в обязанность которых входит хранение сообщений, передаваемых абонентами в течение трех лет, что требует особой организации с технической стороны.

Минцифры внесло предложение о расширении действия «закона Яровой» и на технологические сети крупных компаний, в том числе «Лукойл», РЖД, «Газпром» и др. Данное предложение подверг критике Российский союз промышленников и предпринимателей, заявив, что это значительно увеличит расходы компаний. Мнение Союза поддерживает и Ассоциация предприятий компьютерных и информационных технологий.

Следует отметить, что нормативно-правовая база в области противодействия терроризму и экстремизму в глобальном информационном пространстве на данный момент является эффективным инструментом в борьбе с вышеуказанными явлениями, но вместе с тем, возникает комплекс юридических и технических проблем, которые требуют решения.

2.2. Технические подходы противодействия распространению экстремистской идеологии в сети Интернет

Современные информационно-коммуникационные технологии, в частности сеть Интернет и различные социальные сети, являются невольной «афишей» или своего рода площадкой для рекламы радикально настроенных неформальных организаций, особенно молодёжи. Поэтому противодействие распространению радикальных идей и экстремистской идеологии в сети Интернет является сегодня одним из наиболее актуальных направлений деятельности правоохранительных органов.

Основная проблема противодействия экстремизму в сети Интернет во многом объясняется наличием у преступных сообществ значительного научно-технического потенциала, поскольку они привлекают в свои ряды целые группы квалифицированных специалистов в области высоких технологий.

В настоящее время, подразделениями по противодействию экстремизму ведется мониторинг сети Интернет, а также различных социальных сетей с целью обнаружения экстремистских материалов и различного рода запрещенной информации.

Поводом для начала проведения оперативно-розыскных мероприятий, в процессе поиска контента в сети Интернет, содержащего информацию экстремистского характера могут служить:

− сообщения пользователей об обнаружении Интернет-контента, содержащего материалы экстремистского характера;

− сообщения организаций, предоставляющих услуги информационного характера, о регистрации сайтов, на которых размещена информация экстремистской направленности;

− сведения об обнаружении на российских серверах Интернет-ресурсов, содержащих информацию экстремистской направленности, представленные правоохранительными органами зарубежных стран;

− результаты мониторинга сети Интернет сотрудниками правоохранительных органов.

Однако следует отметить, что процедура внесения сайтов в единый реестр Интернет-ресурсов, запрещенных законом до-

вольно трудоёмкая и не всегда эффективная. Дело в том, что в соответствии с ФЗ №149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», для того чтобы внести определенный сайт в реестр запрещенных законом Интернет-ресурсов, необходимо пройти определенный перечень процедур, который может продлиться несколько суток. К сожалению, довольно часто, этого времени бывает достаточно, чтобы данный Интернет-ресурс выполнил свои задачи.

Мониторинг социальных сетей, распространяющих запрещённую информацию, тоже имеет свои особенности: например, новый пользователь может создать страницу за несколько минут, и также быстро удалить эту страницу. Причем для ее создания пользователю не нужно получать доменное имя как в случае с созданием сайта. В настоящее время очевидно, что необходимо усиливать мониторинг запрещенной информации, распространяющейся в популярных социальных сетях. Следует отметить, что некоторые социальные сети, например «ВКонтакте», сотрудничают с правоохранительными органами по вопросам удаления и блокировки материалов, содержащих запрещенную информацию.

В настоящее время в области противодействия экстремизму и терроризму в глобальном информационном пространстве актуальными и проблемными являются вопросы технического плана.

К ним относятся:

− идентификация личности, разместившей материалы экстремистского или террористического характера;

− идентификация пользователя как автора материала террористической или экстремистской направленности, а не как владельца средств вычислительной техники, с помощью которых в глобальной сети был размещен данный материал.

По мнению экспертов, к одной из эффективных мер по ликвидации анонимности в сети Интернет, является всеобщая персонификация, предполагающая внесение паспортных данных пользователей при регистрации в социальных сетях и различных Интернет-ресурсах.

В настоящее время в РФ применяется подобный порядок регистрации пользователей, однако на данный момент затрагивает только Единый портал государственных и муниципальных услуг.

Условия регистрации на сайте Госуслуг предполагают заполнение анкеты с указанием паспортных данных, СНИЛС, номера мобильного телефона, электронной почты и т. д. После заполнения анкеты необходимо пройти процедуру аутентификации для подтверждения учетной записи. Также возможно получение электронной подписи, которая подтверждает, что сообщение или документ отправлены конкретным человеком.

Однако следует указать, что в целях достижения эффективности данной меры, процесс персонификации должен стать всеобъемлющим. При этом введение этой меры требует комплексного подхода и детальной проработки с участием экспертов в юридической области и специалистов в области IT-технологий. Учитывая то, что процесс персонификации предполагает запрет на анонимность в глобальной сети Интернет, необходимо учесть вопросы соблюдения прав и законных интересов граждан, которые закреплены в статье 29 Конституции РФ. Нужно отметить, что процесс персонификации пользователей в глобальном информационном пространстве, кроме противодействия проявлениям экстремизма и терроризма в киберпространстве, будет способствовать минимизации распространения других запрещенных материалов, например различного рода деструктивной и психотравмирующей информации.

Одной из стран, законодательно реализовавшей данную меру стала КНР, которая с целью защиты суверенитета киберпространства и национальной безопасности страны, усилила контроль и ввела запрет на анонимность в глобальной сети, приняв Закон о кибербезопасности КНР. Указанный нормативный акт стал базовым элементом для государственного регулирования глобальной сети Интернет в части создания, использования и обслуживания глобального информационного пространства, в том числе социальных сервисов. Новые правила регулирования киберпространства, введенные в КНР, вызывали большой интерес и в других информационно развитых стран, для которых борьба с киберугрозой сегодня весьма актуальна.

Своеобразным источником идей экстремизма стали сегодня социальные сети, в которых образуются закрытые группы, ак-

тивно функционируют сайты, проповедующие расовую, национальную, политическую и религиозную нетерпимости. Если рассматривать способы повышения безопасности социальных сетей, то необходимо признать, что каждый из них приведёт к снижению доходов и, к возможному банкротству социальных сервисов.

К способам защиты социальных сетей от несанкционированного доступа следует отнести следующие:

1. Верификация всех страниц социальной сети. Большинство экстремистов регистрируются в социальных сетях, прикрываясь чужими именами, фамилиями или псевдонимами. Таким образом, к примеру, в социальных сетях каждый день появляются многочисленные «Гитлеры», «Бен Ладены» и другие уже не существующие или ещё живущие радикалы. Если удалить из социальных сетей всех, так называемых, «самозванцев», то уровень безопасности значительно повысится. Для этого достаточно обязать пользователей указывать номер удостоверения личности и пройти стандартную процедуру сверки личных данных, при отказе выполнить данные требования, доступ в социальные сети будет закрыт.

2. Штрафование пользователей социальных сетей за призывы к экстремистским действиям. Для технического осуществления данной меры необходимы специальные программы, которые будут выявлять нарушителей, и отправлять ему оповещение о штрафе по обыкновенной или электронной почте. Взымаемые деньги будут поступать в федеральный бюджет. В МГТУ им. Баумана в 2021 году, была разработана специальная программа для отслеживания новостей связанных с буллингом и разжиганием розни [32]. Данная программа имеет обученный алгоритм поиска, который может находить и вычленять ключевые слова и отслеживать первоисточники публикаций в информационном пространстве. Подобные меры помогут дисциплинировать пользователей социальных платформ и отбить у них желание пропагандировать ненависть.

3. Запрет на пользование социальными сетями определённых категорий осуждённых. Для этого в законодательстве должна появиться статья, запреща-ющая посещать социальные сети осуждённым за конкретные категории пре-ступлений. К примеру, посе-

щать «Twitter» и «Facebook» (запрещены в РФ), не могут педофилы и насильники, состоящие в соответствующем реестре «секспреступников» (National Sex Offenders Registry). Однако даже они легко обходят это правило из-за попустительства модераторов.

Новые правила для различных социальных платформ с возможностью комментирования, введенные в КНР с 1 октября 2017 года, обязали всех пользователей проходить процедуру аутентификации личности.

Следует отметить, что значительная часть Интернет-ресурсов несмотря на то, что ориентированы сугубо на российских пользователей, физически и юридически расположены за пределами Российской Федерации, и эта одна из проблем в области технического противодействия экстремизму и терроризму в информационном пространстве. Данная ситуация также осложняется и тем, что экстремисты, как правило, используют хостинги ряда государств, которые не отличаются позитивным отношением к России. Это создает дополнительные трудности для российских правоохранительных органов, осуществляющих поиск информационных экстремистов и пресечение их противоправной деятельности.

Актуальным является вопрос о специализированной подготовке сотрудников подразделений системы МВД, осуществляющих деятельность по противодействию информационному экстремизму. Исследователями в данном направлении отмечается отсутствие надлежащей квалификации сотрудников ОВД, ведущих борьбу с экстремистскими проявлениями в киберпространстве и необходимости расширения их технических возможностей. Для повышения эффективности подготовки квалифицированных кадров в области противодействия экстремизму и терроризму в соответствии с Приказом МВД России от 29.08.2012 № 820 за Краснодарским университетом МВД России и ВИПК МВД России был закреплен профиль подготовки сотрудников ОВД РФ «Деятельность подразделений по противодействию экстремизму, терроризму и борьбе с организованной преступностью». В данных образовательных организациях осуществляется подготовка квалифицированных кадров для подразделений по противодействию экстремизму и терроризму. Разработка программ обучения по данному направлению осуществляется во взаимосвязи с ГУПЭ МВД

России, ГУОООП МВД России, ГУУР МВД России. Учитывая актуальность угрозы информационного экстремизма в глобальном информационном пространстве, в программах обучения предусмотрено владение сотрудников полиции компетенциями по решению следующих вопросов:

− информационное противоборство в сфере борьбы с терроризмом;

− противодействие использованию информационно-телекоммуникационных сетей (включая сеть Интернет) в террористической деятельности.

В учебном процессе предусмотрено использование научных разработок в области противодействия идеологии экстремизма и проявлений терроризма в информационном пространстве, что позволит обеспечить высокий уровень подготовки сотрудников полиции в соответствии с современными требованиями.

Органы государственной власти уделяют большое внимание проблемам обеспечения технического противодействия экстремизму в сети Интернет. Об этом говорят вносимые поправки в законодательные акты РФ. В целях повышения эффективности работы подразделений системы МВД России по противодействию экстремизму, образовательными организациями МВД России проводится подготовка квалифицированных кадров в данной области. Однако, с учетом особенностей экстремизма и терроризма в глобальном информационном пространстве возникает ряд юридических и технических проблем, связанных с доработкой нормативно-правовой базы в данной области, введением процесса всеобщей персонификации, организации надежной системы сотрудничества и взаимодействия с правоохранительными органами зарубежных стран.

2.3. Методы противодействия кибератакам, направленным на дестабилизацию информационных инфраструктур государства

Одним из важных направлений работы по защите информационного пространства от преступной деятельности экстремистских организаций является противодействие хакерам, которые привлекаются экстремистами для совершения атак на автоматизированные системы управления государств и информационно-телекоммуникационные сети. Как отметили в Национальном координационном центре по компьютерным инцидентам, в связи со сложившейся геополитической обстановкой в настоящее время существуют большой риск компьютерных атак на российские информационные ресурсы, в том числе на объекты критической информационной инфраструктуры.

Наиболее важное место среди субъектов обеспечения информационной безопасности отводится государству, поскольку именно оно владеет всем спектром средств, необходимых для обеспечения национальной безопасности в информационной сфере. Защита национальных интересов России от угроз как внешнего, так и внутреннего характера в информационной области является основным направлением деятельности государства по обеспечению информационной безопасности.

Вопросы защиты информации в Российской Федерации возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК), которая сменила Гостехкомиссию РФ. Требования, которые были разработаны ФСТЭК еще в 2010-х годах, являлись обязательными к использованию, но, по мнению специалистов, предельно техническими и мало учитывающими управленческие и организационные вопросы при обеспечении информационной безопасности.

В соответствии с указом Президента РФ от 22 декабря 2017 года № 620, функции предупреждения, обнаружения и ликвидации последствий компьютерных атак возложены на Федеральную службу безопасности Российской Федерации.

В соответствии с данным указом одной из задач государственной системы предупреждения и ликвидации последствий кибератак (ГосСОПКА) на информационные ресурсы РФ является контроль степени защищённости информационных ресурсов РФ от кибератак. К средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий кибератак и реагирования на компьютерные инциденты относятся:

− технические;

− программные;

− программно-аппаратные и иные средства.

Указанные средства используются для обнаружения (поиска признаков компьютерных атак в сетях электросвязи, обеспечивающих взаимодействие объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий кибератак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

В 2021-2023 годах многие российские компании и интернет-сайты, а также некоторые министерства и ведомства подвергались массированным кибератакам. Так в июле 2023 года официальные сайты Министерства обороны РФ и Росгвардии подверглись массированной DDoS-атаке.

По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации 10 ноября 2021 года была отражена максимальная по мощности (превысила 680 Гигабит в секунду) атака на портал «Госуслуги». Часть пользователей испытывали временные проблемы с доступом к порталу госуслуг, в официальном сообщении на сайте отмечалось, что он недоступен по техническим причинам. Позднее стало известно компания «Яндекс» также подверглась самой крупной DDoS-атаке в истории российского интернета.

Приказом ФСБ России от 24.07.2018 № 366 был создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ), основными задачами которого являются обнаружение и ликвидация кибератак. НКЦКИ положил начало единой системе

предупреждения и защиты критической информационной инфраструктуры от хакерских атак и устранения их негативных последствий.

Сегодня обеспечение информационной безопасности автоматизированных систем является динамично развивающейся областью, охватывающей помимо правовых, криптографические, математические, программно-аппаратные, технические и организационные аспекты обеспечения безопасности информации.

Условно системы информационной безопасности можно разделить на две категории:

− системы предотвращения угроз (управления доступом);

− системы мониторинга активности.

Первые управляют обеспечением конфиденциальности, целостности и доступности ценной информации, осуществляют автоматизацию процессов защиты данных с учетом всех ограничений, типов информационных ресурсов и пользователей.

Вторая категория систем обеспечивает только мониторинг, следит за угрозами и проблемами, обнаруживает их и уведомляет службы безопасности.

Системы мониторинга активности в свою очередь, подразделяются на следующие виды:

− система анализа конфигураций оборудования, правил доступа сетевого оборудования;

− система обнаружения компьютерных атак и сетевых аномалий;

− система пассивного анализа уязвимостей;

− система контроля целостности данных и программного обеспечения;

− система мониторинга событий информационной безопасности и беспроводных сетей.

Классификация систем информационной безопасности по направлению их использования предполагает деление на следующие две категории:

− традиционные;

− специализированные.

Первая категория систем ИБ может использоваться на промышленных предприятиях. Их назначение – управление информационными потоками и построение архитектуры ИБ.

Вторая категория систем ИБ непосредственно предназначены для компаний тяжелой промышленности (металлургическая, нефтегазовая и энергетическая промышленность). Для них характерна более агрессивная среда: температура, магнитные излучения, пыль. Специализированные системы безопасности учитывают специфические требования, применение специального монтажа промышленного оборудования, имеют устойчивость к агрессивным средам.

Проведенный анализ критически важных информационных систем показывает, что используемые средства для предотвращения кибератак должны обладать распределенной структурой компонентов. Данные компоненты будут интегрированы в качестве датчиков в информационное и программное обеспечение, что обеспечит мониторинг кибератак и их предупреждение на ранней стадии в процессе реализации технологического цикла управления.

Организацию эффективного функционирования средств противодействия компьютерным атакам возможно обеспечить только при комплексном и взаимосвязанном использовании средств защиты от несанкционированного доступа, антивирусных средств и межсетевых экранов. Особое внимание необходимо обратить на согласованность работы средств противодействия компьютерным атакам с администраторами вычислительной сети и безопасности информации.

Важным направлением при обеспечении ИБ является развитие технологий безопасности на отечественных платформах, которое дало бы возможность исключить заимствование и принятие готовых решений со стороны западных компаний, являющихся источником постоянной уязвимости и зависимости.

В связи с новыми вызовами и угрозами, направленными на критическую информационную инфраструктуру Российской Федерации, Президентом России издан указ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30

марта 2022 года № 166. В соответствии с ним, с 31 марта 2022 г. заказчики, осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры РФ. С 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры. В соответствии с указом Правительству РФ даны, в том числе, поручения: обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для критической информационной инфраструктуры; организовать подготовку и переподготовку кадров в сфере разработки, производства, технической поддержки и сервисного обслуживания радиоэлектронной продукции и телекоммуникационного оборудования.

Таким образом, можно заключить, что проблема противодействия хакерским атакам, в частности, направленным на дестабилизацию критически важных информационных систем РФ, сегодня является одной из первостепенных задач органов государственной власти. Актуальность проблемы подтверждает рост количества кибератак на системы управления критически важными инфраструктурами государства, включая военную сферу, ядерную и топливную энергетику, системы опасных производств, что может повлечь за собой дестабилизацию государства, огромные материальные потери, экологические катастрофы, глобальные жертвы и разрушения.

Угроза кибертерроризма сегодня остаётся весьма актуальной, а ее эффективное преодоление возможно только совместными усилиями всех стран с развитой информационной инфраструктурой на основе принципов планомерности и системного подхода.

2.4. Информационные технологий, направленные на профилактику экстремизма в сети Интернет

Содержание веб-материалов экстремистского толка отличается хорошей теоретической базой, проработанным спектром способов управляемого информационно-психологического воздействия на массовое сознание и высокой защищенностью ресурсов. В силу этого, вопросы информационного противодействия проявлениям экстремизма и терроризма в сети Интернет, которая активно используется преступниками для информационного обеспечения своей противоправной деятельности, сегодня весьма актуальны, что отмечено в законодательной базе РФ.

К основным мерам информационного противодействия относятся информационно-пропагандистские меры, которые направлены на выявление сущности и организацию разъяснительной работы об опасности различных проявлений экстремизма и терроризма, осуществлению воздействия на сознание граждан в целях формирования неприятия идеологии насилия, жестокости и привлечения их к участию в противодействии экстремизму и терроризму. Поэтому сегодня одной из наиболее важных задач органов государственной власти является активизация противодействия распространению идеологии экстремизма и терроризма и организация информационно-пропагандистского обеспечения в целях осуществления антиэкстремистских и антитеррористических мероприятий в едином мировом информационном пространстве.

Среди целей, задач и основных направлений государственной политики в сфере противодействия экстремизму в «Стратегии противодействия экстремизму в Российской Федерации до 2025 года» (утв. Президентом РФ 28.11.2014), и терроризму в «Концепции противодействия терроризму в Российской Федерации» (утв. Президентом РФ 5 окт. 2009 г.), в том числе, указаны:

– проведение тематических встреч с представителями средств массовой информации и Интернет-сообщества в целях противодействия распространению идеологии экстремизма;

– подготовка и размещение в средствах массовой информации, в информационно-телекоммуникационных сетях, включая

сеть Интернет, социальной рекламы, направленной на патриотическое воспитание молодежи;

– разъяснение сущности терроризма и его общественной опасности, формирование стойкого неприятия обществом идеологии насилия, а также привлечение граждан к участию в противодействии терроризму;

– координация осуществления мер информационного противодействия распространению экстремистской идеологии в информационно-телекоммуникационной сети Интернет (в том числе в социальных сетях), а также проведение на системной и регулярной основе работы с привлечением видных деятелей культуры, науки, авторитетных представителей общественности, информационного сообщества, конфессий и национальных общин по разъяснению сути противоправной деятельности лидеров экстремистских организаций;

– противодействие распространению идеологии терроризма путем обеспечения защиты единого информационного пространства Российской Федерации;

– совершенствование системы информационного противодействия терроризму.

Для осуществления мониторинга состояния общегосударственной системы противодействия терроризму указом Президента РФ от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» был образован Национальный антитеррористический комитет (НАК). Указом Президента РФ от 26 декабря 2015 г. № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму» утверждено Положение о Национальном антитеррористическом комитете. НАК координирует деятельность федеральных органов исполнительной власти в области информационно-аналитической работы по проблемам противодействия терроризму и организует подготовку информационно-аналитических материалов по проблемам, требующим межведомственной экспертной оценки и обсуждения на заседаниях Комитета. Комитет обобщает справочную и отчетную информацию субъектов противодействия терроризму для подготовки ежегодного итогового доклада Президенту Россий-

ской Федерации. НАК, в состав которого входят руководители федеральных органов исполнительной власти, согласовывает деятельность по противодействию терроризму на федеральном, региональном и местном уровнях посредством законодательно созданных коллегиальных органов.

Сайт НАК, размещенный по адресу http://nac.gov.ru/, обеспечивает организацию информирования населения о возникновении и нейтрализации угроз террористической направленности, содержит материалы, ориентированные на системную профилактическую работу по неприятию в обществе идеологии терроризма и экстремизма. На сайте размещены сведения о целях, задачах, структуре НАК, законодательной базе, публикациях в области противодействия терроризму и экстремизму, информация о мероприятиях, осуществляемых в рамках международного сотрудничества, о проведенных и планируемых конференциях, круглых столах, брифингах и т.п.

В сентябре 2023 года в Москве на площадке Центра международной торговли была проведена Международная конференция по проблеме распространения идеологии экстремизма, организованной МВД России.

В мероприятии приняли участие заместитель Министра внутренних дел Российской Федерации генерал-полковник полиции Андрей Храпов, начальник Главного управления по противодействию экстремизму МВД России генерал-лейтенант полиции Олег Ильиных, начальник НЦБ Интерпола МВД России генерал-майор полиции Валерий Калачев и другие.

Заместитель Министра отметил, что органы внутренних дел Российской Федерации накопили достаточный опыт по предупреждению, выявлению и раскрытию преступлений экстремистского характера. Поэтому даже в период санкций и запретов наша страна успешно защищает свои интересы.

Среди выступивших на конференции – представители Республики Абхазия, Социалистической Республики Вьетнам, Китайской Народной Республики, Республики Кыргызстан, Республики Союз Мьянма, Республики Сербия, Сирийской Арабской Республики, Республики Судан, Республики Таджикистан. Зарубежные

коллеги изложили свое видение ситуации в сфере противодействия экстремизму и поделились опытом соответствующей деятельности.

Участники конференции выразили озабоченность по поводу нарастающего использования современных информационно-коммуникационных технологий в целях внедрения в массовое сознание людей идеологии экстремизма, отметили особую опасность попыток возрождения идеологии нацизма и героизации ее последователей, обозначили намерение препятствовать политизации международного полицейского сотрудничества.

В мае 2024 года в Москве во Всероссийском научно-исследовательском институте Министерства внутренних дел Российской Федерации прошла вторая Международная научно-практическая конференция по теме «Актуальные проблемы противодействия экстремизму и терроризму»

Проведение этой конференции стало уже традицией, она получила название «Сундиевские чтения» в честь доктора философских наук, профессора Игоря Сундиева, который глубоко изучал корни терроризма. Для участия было подано более 100 заявок и 50 докладов, в том числе от ученых и практиков, работников правоохранительных органов из дружественных иностранных государств. Эксперты говорили об особых видах экстремизма и терроризма. Так, советник министра внутренних дел Владимир Овчинский обозначил современные тенденции: появление неовласовцев (русских, воюющих против своей страны), выделение молодежи, как одиночек, так и в группах, экстремистского настроя и псевдоигиловское движение среди мигрантов [33].

На сайте Общественной палатой РФ, размещенной по адресу https://www.oprf.ru/1449/2134/2205/2206/ открыта Интернет-приемная (рис. 4), в которой граждане могут отправить обращение в случае, если у них имеются опасения, что их близкие могли быть подвергнуты влиянию вербовщиков экстремистских группировок.

Анализ и обобщение имеющегося положительного опыта в области противодействия идеологиям экстремизма и терроризма в сети Интернет показывает, что для того, чтобы эффективно предупреждать его влияние на наиболее подверженные категории лю-

дей, в первую очередь молодежь, необходимо создание и функционирование на постоянной основе доступного и популярного для подрастающего поколения Интернет-контента, который обеспечивал бы возможность ведения откровенного онлайн-диалога в понятной и привычной для молодых людей манере.

В настоящее время в сети Интернет по инициативе студентов, профессорско-преподавательского состава и ученых образовательных и научных учреждений с целью информационного противодействия экстремизму и терроризму в сети Интернет созданы и эффективно работают следующие Интернет-ресурсы:

– портал «Наука и образование против террора» (http://www.scienceport.ru/), главной задачей которого является интеграция ученых, преподавателей и студентов российских вузов с целью оказания научного противодействия насилию и террору. Сегодня портал включает 258 образовательных учреждений и организаций РФ;

– сайт «Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет» (НЦПТИ) (http://нцпти.рф/), к одной из ключевых задач которого относится профилактика распространения экстремистской идеологии в киберпространстве. Сайтом НЦПТИ организованы курсы онлайн-обучения: «Сеть Интернет в противодействии террористическим и экстремистским угрозам», «Интернет без угроз. Практикум для родителей», «Курс для киберволонтеров»;

– большой вклад в вовлечение молодежи в общественно-значимую деятельность по профилактике терроризма и экстремизма в сети Интернет вносят мероприятия, проводимые образовательными учреждениями совместно с НЦПТИ. Так, с 2017 года ежегодно проводится Всероссийский онлайн-фестиваль социальных видеороликов «Я против экстремизма», глав-ной задачей которого было повышение роли молодежных сообществ в профилактике террористической идеологии, способности противостоять террористическим угрозам, а также формирование информационной базы с целью противодействия распространения идей терроризма и экстремизма в молодежной среде и Интернете.

Активно используются блоги на сторонних площадках, так на видео-сервисе «YouTube» размещено более 10000 видеороликов антиэкстремистской и антитеррористической направленности.

В рамках реализации основных направлений государственной политики в сфере противодействия экстремизму и терроризму, следует отметить положительный опыт проведения Интернет-семинаров в целях обсуждения актуальных проблем противодействия идеологии экстремизма и терроризма с использованием возможностей глобального информационного пространства. Возможности для увеличения масштабов аудитории при этом практически безграничны и определяются предварительным информированием потенциальных участников Интернет-семинаров.

Как отмечено в законодательной базе, а также специалистами по противодействию экстремизму и терроризму в сети Интернет, надлежит активнее применять возможности социальных сервисов для проведения на регулярной основе активных пропагандистских и контрпропагандистских акций. При этом целесообразно поддерживать уважительный и корректный формат взаимоотношений с активными блогерами, которые инициативно готовы оказывать помощь государству и обществу для осуществления информационного противоборства с идеологами экстремизма и терроризма. Так, в популярной социальной сети «ВКонтакте» действует страница портала «Наука и образование против террора» размещенная по адресу (https://vk.com/net_terroru).

В целях актуализации материалов с антитеррористическим контентом, которые ориентированы на категоричное неприятие идеологии экстремизма и терроризма, а также для формирования контрпропагандистских призывов и лозунгов, выбора наиболее эффективной методики и приемов ведения диалога и полемики надлежит активно использовать возможности созданных экспертно-консультативных советов и действующих на постоянной основе рабочих групп по информационному противодействию идеологии терроризма и экстремизма.

Необходимо отметить, что в настоящее время требуется совершенствование координации мероприятий по противодействию идеологиям терроризма и экстремизма в сети Интернет. Несмотря на то, что в каждом регионе функционирует немалое количество

информационных площадок, которые содержат сайты образовательных и общественных организаций, на которых размещены соответствующие антиэкстремистские и антитеррористические материалы, однако все это происходит бессистемно и спонтанно. В целях увеличения эффективности предпринимаемых мер информационного противодействия требуется интеграция соответствующих мероприятий под эгидой территориальных образовательных организаций совместно с антитеррористическими комиссиями. У молодого поколения необходимо воспитать толерантное отношение к представителям других народов, культур и религий, чтобы они в последующем не стали целью экстремистов.

При этом большая ответственность за воспитание несовершеннолетних, в том числе осуществление контроля за использованием ими глобального информационного пространства, лежит на родителях, которые зачастую недооценивают потенциальную угрозу, которую несёт их детям киберпространство. Активное использование Интернет-ресурсов, особенно социальных сервисов, может погрузить несовершеннолетнего пользователя в негативную среду, способствующую заполнению возникшего в последнее время идеологического «вакуума» догмами и установками терроризма и экстремизма. Пресс-службой ФСБ России настоятельно рекомендуется родителям наблюдать за активностью детей в социальных сетях и сообщать по телефонам доверия о потенциальных угрозах национальной безопасности Российской Федерации. Компанией «Лаборатория Касперского» разработано специальное программное приложение «Kaspersky Safe Kids», устанавливаемое на мобильный телефон ребёнка, которое позволяет заблокировать нежелательные сайты и приложения, быть в курсе его публикаций и изменений в списке друзей в социальных сервисах, знать о подозрительных группах, в которых состоит ребенок.

Сегодня многие работодатели устанавливают запрет на использование социальных сетей своими сотрудниками, чтобы воспрепятствовать утечке информации, которая вводится пользователем при регистрации на сайте. Данная информация затем используется экстремистскими и террористическими сообществами для

анализа личности регистрируемого пользователя, с целью определить его отношение к той или иной проблеме, с последующей возможностью его вовлечения в преступную деятельность.

Не стоит ущемлять огромную роль религиозных организаций в борьбе с терроризмом, так как только служители культа смогут наиболее грамотно разъяснить населению основы религии и выявить его искажения. В целях донесения до пользователей глобальной сети Интернет достоверной информации о позиции мусульманского сообщества в отношении экстремизма и терроризма, противодействия террористической и экстремистской деятельности, ее социально-экономических и культурологических аспектах создан сайт «Ислам против терроризма», размещенный по адресу http://terrora-net.ru/.

Таким образом, можно отметить, что только совместная конструктивная деятельность органов государственной власти, образовательных, научных, общественных и религиозных организаций в общем, а также каждого сознательного гражданина в отдельности, способна результативно противодействовать распространению экстремистских взглядов и террористических идей в глобальной сети Интернет.

Заключение

Глобальная информатизация практически всех сфер жизнедеятельности общества повлекла за собой снижение степени его безопасности. Экстремизм в сети Интернет на современном этапе способен стать причиной системного кризиса в любом государстве, имеющем высокоразвитую информационную инфраструктуру. В данных условиях уязвимость критической информационной инфраструктуры перестает оставаться проблемой государства в отдельности, а представляет собой глобальную мировую угрозу, противостоять которой возможно только общими усилиями, на основе системы коллективной информационной безопасности с учетом современных требований.

Решение данной задачи требует не только принятия соответствующих законодательных актов на национальном уровне, но и разработку единых международных стандартов, определяющих унификацию понятийного аппарата, дефиницию круга деяний, подлежащих криминализации, имплементации международных норм в национальное уголовное право.

Проявление экстремизма отмечается в различных сферах общественной жизни, в том числе: социальной и религиозной, политической и экономической. Экстремистские идеологи активно используют в своих преступных целях несовершенство законодательной базы, достижения технического прогресса.

Вместе с созданием и поддержанием собственных Интернет-сайтов экстремистские организации проявляют высокую активность на форумах, в социальных сетях, порталах общего доступа, осуществляют вербовку новых сторонников в свои ряды, что подтверждается мнением специалистов, которые отмечают, что «бесконтактные» вербовки во всемирной сети сегодня приобрели глобальный характер.

Экстремистами также активно используются программно-математические методы информационного оружия, которые предполагают создание средств опасного воздействия на информационные сферы государства; нарушение нормального

функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Необходимо отметить, что целью экстремистов является оказание разрушительного воздействия на системы управления критически важными инфраструктурами государства: военной сферы, ядерной энергетики, системами вредных и опасных производств, системами управления транспортными средствами, финансовыми и другими информационными системами государства [34].

В связи с этим, в настоящее время, одной из приоритетных задач органов государственной власти является разработка и внедрение эффективных технологий, направленных на противодействие проявлениям экстремизма в сети Интернет.

Нормативно-правовая база в области противодействия терроризму и экстремизму в глобальном информационном пространстве на данный момент является эффективным инструментом в борьбе с вышеуказанными явлениями, но вместе с тем, возникает комплекс юридических и технических проблем, которые требуют решения.

К способам защиты социальных сетей от несанкционированного доступа следует отнести следующие: верификация всех страниц социальной сети, штрафование пользователей социальных сетей за призывы к экстремистским действиям, запрет на пользование социальными сетями определённых категорий осуждённых.

Необходимо отметить, что органы государственной власти уделяют большое внимание проблемам обеспечения технического противодействия экстремизму в глобальном информационном пространстве. Об этом говорят вносимые поправки в законодательные акты РФ. Однако, с учетом особенностей экстремизма и терроризма в глобальном информационном пространстве возникает ряд юридических и технических проблем, связанных с доработкой нормативно-правовой базы в данной области, введением процесса всеобщей персонификации, организации надежной системы сотрудничества и взаимодействия с правоохранительными органами зарубежных стран.

Угроза кибертерроризма сегодня остаётся весьма актуальной, а ее эффективное преодоление возможно только совместными усилиями всех стран с развитой информационной инфраструктурой на основе принципов планомерности и системного подхода.

Основополагающей частью в системе противодействия идеологии экстремизма и терроризма в глобальном информационном пространстве должна стать информационно-пропагандистская работа, осуществляемая как государственными службами, так и иными организациями в сети Интернет. Профилактическая деятельность, осуществляемая в целях формирования антитеррористического и антиэкстремистского сознания населения, должна основываться на принципах постоянства, систематичности, комплексности. К профилактической работе необходимо привлекать практических работников, занимающихся проблемами противодействия данным противоправным явлениям, научных деятелей, психологов, педагогов, студентов высших учебных заведений, общественных экспертов и представителей организаций.

В современных условиях противостояния с Западом отмечены следующие установки Российской Федерации по вопросам международного сотрудничества в борьбе с терроризмом:

– необходимость опоры антитеррористического сотрудничества на выработанную международно-правовую базу, признание ведущей роли государств и их компетентных органов в борьбе с терроризмом;

– недопустимость использования данной проблематики, как и самих террористических группировок, в качестве инструмента геополитики и вмешательства во внутренние дела, дестабилизации «неугодных» Западу режимов.

В работе рассмотрены различные способы использования широких возможностей сети Интернет экстремистскими организациями, а также методы и технологии противодействия информационному экстремизму. Однако продолжающаяся мировая информационно-технологическая революция создает новые потенциальные угрозы жизнедеятельности как государств, так

и мирового сообщества в целом. В наибольшей степени это относится к экстремизму и терроризму, мутация которых, по мнению экспертов, происходит именно в информационной сфере. Поэтому эффективное решение данной проблемы требует координации усилий по дальнейшему совершенствованию технических средств и разработке новых методов информационного противодействия деятельности экстремистских организаций в глобальном информационном пространстве.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.04.2024).

3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 22.04.2024).

4. Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 30.06.2018): федер. закон от 27 июля 2006г. № 149-ФЗ (ред. от 14.07.2022) // Рос.газ. – 2006. – № 165.

5. Об общественных объединениях (с изменениями и дополнениями): федер. закон от 19 мая 1995 № 82-ФЗ // СПС «КонсультантПлюс» (дата обращения: 20.04.2024).

6. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 06 июля 2016 г. № 374-ФЗ // Рос.газ. – 2016. – № 149.

7. Министерство юстиции Российской Федерации. [Электронный ресурс]. – Режим доступа: https://minjust.gov.ru/ru/extremist-materials/ (дата обращения: 08.05.2024).

8. О противодействии экстремистской деятельности (с изменениями и дополнениями) федер. закон от 25 июля 2002 № 114-ФЗ // СПС «КонсультантПлюс» (дата обращения: 20.04.2024).

9. Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года».

10. Об архивном деле в Российской Федерации (ред. от 11.06.2021): федер. закон от 22 нояб. 2004г. № 125-ФЗ // Рос.газ. – 2004. – № 237.

11. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 06 июля 2016 г. № 375-ФЗ // Рос.газ. – 2016. – № 150.

12. В России каждое третье преступление экстремистской направленности совершается через Интернет. [Электронный ресурс]. URL: https://www.1tv.ru/news/2024-04-24/475494 (дата обращения: 12.05.2024).

13. Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими. [Электронный ресурс]. URL: http://www.fsb.ru/fsb/npd/terror.htm (дата обращения: 12.05.2024).

14. 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]. URL: https://minjust.gov.ru/ru/documents/7822/ (дата обращения: 12.05.2024).

15. Вся статистика интернета и социальных сетей на 2023 год — цифры и тренды в мире и в России. [Электронный ресурс]. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/. (дата обращения: 12.05.2023).

16. . Ожегов С.И. Толковый словарь русского языка / под ред. Л.И. Скворцова. –М., 2009. – 1340 с.

17. Устинов, В.В. Обвиняется терроризм / М.: Издательство Олма-Пресс, 2002. – 416 с.

18. Coleman P.T., Bartoli A. Addressing Extremism. The International Center for Cooperation and Conflict Resolution (ICCCR), Teachers College, Columbia Uni-versity / The Institute for Conflict Analysis and Resolution (ICAR), George Mason University, 2002. P. 2.

19. Хлебушкин А.Г. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации. М., 2010. – С. 25-29.

20. Бирюков В.В. В отношении изменений, внесенных в Федеральный закон №114-Фз «О противодействии экстремисткой деятельности» // Военно-юридический журнал. 2007. – №12. – С. 22-25.

21. Власов В.И. Экстремизм: сущность, виды, профилактика: учеб.-метод. пособие. М., 2003. С. 8-10.

22. Экстремизм представлен в основном возрастной группой. Молодежный экстремизм как одна из наиболее актуальных социально – политических проблем в России. [Электронный ресурс]. – Режим доступа https://not-not.ru/eda/ekstremizm-predstavlen-v-osnovnom-vozrastnoigruppoi.html (дата обращения: 12.05.2024).

23. О стрельбе в российских школах: история и хронология. [Электронный ресурс]. – Режим доступа: https://news.ru/society/o-strelbe-v-rossijskih-shkolah-istoriya-i-hronologiya/ (дата обращения: 12.05.2024).

24. Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ от 28 нояб. 2014г. № Пр-2753) / Правовая база http://www.scrf.gov.ru (дата обращения: 12.05.2024).

25. Жукова О.С. Информационный экстремизм в современном государственно – правовом государстве [Текст] / О. С. Жукова, Р. Б. Иванченко, В. В. Трухачёв. – Философия права. – Изд-во: Ростовский юридический институт МВД, 2010. – С. 105 -108.

26. Бесконтактная вербовка: как террористы заманивают молодежь через соцсети. РИА Новости. [Электронный ресурс]. Режим доступа URL: https://ria.ru/society/20180228/1515459761.html (дата обращения: 10.05.2024).

27. Сундиев И.Ю. Трансформация роли политического и религиозного экстремизма в условиях развертывания глобального кризиса // Актуальные проблемы противодействия национальному и политическому экстремизму: Материалы Всероссийской научно-практической конференции. В 2-х т. / Под ред. А.-Н. З. Дибирова, М. Я. Яхьяева, А. М. Муртазалиева, К. М. Ханбабаева. — Махачкала: Издательство «Лотос», 2008. –Т. 1. – 384 с.

28. Шогенов Т.М. Об актуальных вопросах пресечения деятельности радикальных сообществ, вовлекающих молодежь в совершение преступлений террористической направленности /

Т.М. Шогенов, Л.А. Бураева, А.Н. Кучмезов // Евразийский юридический журнал, 2022. –№ 2 (165). – С. 448-450.

29. Источник рассказал, как вербовали террористов, напавших на «Крокус» [Электронный ресурс] – Режим доступа URL: https://ria.ru/20240327/terakt-1936270949.html?ysclid=lw69djouo911955930 (дата обращения: 11.05.2024).

30. Число кибератак в России и в мире. [Электронный ресурс]. – Режим доступа: Число кибератак в России и в мире (tadviser.ru) (дата обращения: 08.05.2024).

31. Данные судебной статистики. [Электронный ресурс]. URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 05.05.2024).

32. По ключевым словам: в Российской Федерации создали программу для выявления травли в сети. [Электронный ресурс]. – Режим доступа: https://iz.ru/1127203/mariia-frolova/po-kliuchevym-slovam-v-rossii-sozdali-programmu-dlia-vyiavleniia-travli-v-seti (дата обращения: 04.05.2024).

33. Ученые обсудили методы противодействия терроризму [Электронный ресурс]. – Режим доступа: https://vm.ru/news/1135246-uchenye-obsudili-metody-protivodejstviya-terrorizmu?ysclid=lw7ugyu18i709709786 (дата обращения 14.05.2024).

34. Бураева Л.А. О мерах по обеспечению безопасности автоматизированных информационных систем, в том числе относящихся к системам критической инфраструктуры государства / Л.А. Бураева, С.Н. Архипов // Проблемы экономики и юридической практики, 2019. –Т. 15. –№ 1. С. 186-188.

35. Ксенофобия и экстремизм: глобальные вызовы и региональные тренды: Сборник докладов Международной онлайн-конференции, г. Москва, 26 октября 2021 г: материалы конференции / научный редактор В.В. Энгель. — Москва: Дашков и К, 2022. - 418 с.

36. Организация деятельности правоохранительных органов по противодействию экстремизму и терроризму: учебное пособие / Е.Н. Быстряков, Е.В. Ионова, Н.Л. Потапова, А.Б. Смушкин. - 2-е изд., стер. – Санкт-Петербург: Лань, 2022. - 176 с.

37. Рарог А.И. Уголовно-правовое противодействие терроризму и экстремизму: учебное пособие / А.И. Рарог, В.В. Палий. – Москва: Проспект, 2021. - 96 с.

38. Сахнов И.П. Противодействие распространению идеологии экстремизма и терроризма и профилактика аддиктивного поведения в молодежной среде: учебно-методическое пособие / И.П. Сахнов. – Кострома: КГУ им. Н.А. Некрасова, 2021. – 147 с.

Содержание

Учебное издание

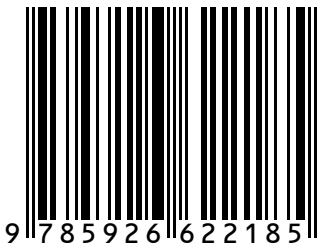
Битов Алим Асламович
Магомедов Мурад Насруллаевич

МЕТОДЫ И ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Методические рекомендации

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2218-5



Подписано в печать 15.09.2025. Формат 60x84 1/16.
Усл. печ. л. 4,0. Тираж 50 экз. Заказ 399.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.