

Н. Г. Дубовик,
*Московский университет МВД России
имени В. Я. Кикотя*

КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ ЭКСТРЕМИСТСКИХ ПРОЯВЛЕНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

CRIMINOLOGICAL ANALYSIS OF EXTREMIST MANIFESTATIONS IN SOCIAL NETWORKS

В статье рассматриваются реальные и потенциальные угрозы экстремистской направленности в информационно-телекоммуникационной среде. Анализируется правоприменительная практика. На основании проведенного исследования предложены меры по борьбе с экстремистскими проявлениями.

The article discusses the real and potential threats of an extremist orientation in the information and telecommunications environment. The law enforcement practice is analyzed. Based on the study, measures were developed to combat extremist manifestations in the Russian Federation.

Одним из основных источников криминологической информации в современном мире является интернет-пространство. Все сферы нашей жизни отражаются в сети Интернет — как в виде использования ее в личных целях: виртуальное общение в социальных сетях, переписка в электронной почте, покупка (продажа) товаров, так и для выполнения служебных обязанностей — государственные (муниципальные услуги); запись в детский сад, школу или поликлинику; документооборот между различными ведомствами и организациями. Как следствие, с каждым годом количество пользователей возрастает. Так, агентством социологических исследований ООО «ФОМ» было выявлено, что в Российской Федерации 50,1% (58,4 млн) населения — активные пользователи сети Интернет, т.е. хотя бы раз в сутки посещают интернет-пространство [1].

Факт увеличения преступлений с применением информационных технологий был отмечен Генеральным прокурором Российской Федерации 10 апреля 2019 года на заседании Совета Федерации. В частности, за 2017 и 2018 годы зафиксировано увеличение данного вида преступления в 2 раза [2].

В процессе интенсивного развития и роста возможностей интернет-ресурсов содержащаяся в них информация перестала быть контролируемой, поэтому в анализируемой сфере существует боль-

шая вероятность наличия деструктивной информации экстремистского характера с пропагандой радикальной идеологии.

Анализ недалекого прошлого и настоящего постсоветского пространства и других регионов мира позволяет определить закономерности того, как с помощью информационных ресурсов были разработаны методы вмешательства в суверенитет [15] и внедрены сценарии «цветных революций» с целью смены социально-политической системы государств, их элиты, а также бесконтрольного доступа «интересантов» к природным и иным ресурсам различных стран и народов.

Актуальность исследуемой темы подтверждается тем, что с каждым годом увеличивается количество лиц, привлекаемых к уголовной ответственности за размещение публичных призывов и высказываний экстремистской направленности с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Такие решения, как правило, имеют большой общественный резонанс. Статистика последних лет свидетельствует, что борьба с экстремизмом переходит из реального мира в виртуальный. Так, в 2015 году их удельный вес был 55,5% (737), в 2016 г. — 65,5% (950), в 2017 г. достиг 75,7% (1151) [3. — С. 550].

В частности, А. В. Петряниным для определения характера и степени общественной опасности

информационной среды как средства совершения преступлений экстремисткой направленности было проведено исследование в виде интервьюирования респондентов, в ходе которого был задан вопрос: «В каких формах Вы наблюдали призывы к экстремисткой деятельности либо распространения экстремистских материалов?» 96% опрошенных ответили, что столкнулись с данной информацией в сети Интернет [4. — С. 159].

Анализ тенденций развития информационно-телекоммуникационных технологий позволяет прогнозировать дальнейшее нарастание объемов использования Интернета экстремистскими сообществами для вовлечения в них радикально настроенных людей.

На сегодняшний день в Российской Федерации насчитывается свыше шестидесяти запрещенных общественных и религиозных объединений и иных некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности («Управленческий центр Свидетелей Иеговы в России», «Меджлис крымскотатарского народа», «АльКаида», ХАМАС (Движение исламского сопротивления), «Хезболла» («Партия Аллаха»), «Аль-Джихад» (Египетский исламский джихад), «Братья-мусульмане» («Аль-Ихван аль-Муслимун»), «Народный фронт освобождения Палестины», «Конграгел» (бывшая Рабочая партия Курдистана), «Революционные вооружённые силы Колумбии» и др.) [5].

Радикальные группы предлагают студентам и школьникам ценностно-смысловую традицию, которой так не хватает в обществе технологий. Если в прошлом столетии экстремистская деятельность была ограничена пределами города, района или области, то сейчас благодаря информационным технологиям становится элементом медийной повестки дня в масштабах страны в режиме реального времени. Спрогнозировать, где, когда и какого рода информация появится в сети, крайне сложно. Интернет становится орудием всеобщего доступа к средствам массовой информации, или, говоря точнее, массовой дезинформации, а также главной средой коммуникации.

Если обратиться к официальным источникам, то можно сделать вывод, что 80% участников экстремистских организаций это лица в возрасте до 30 лет. Так, Е. В. Демидовой-Петровой было проанализировано 330 уголовных дел в период с 2011 по 2018 год. После проведенного исследования было выявлено, что чаще совершают преступления экстремистской направленности подростки в возрасте 13—18 лет. При этом более 80% из них на момент совершения преступления являются

учащимися вузов и средних специальных учебных заведений [6. — С. 478]. Одной из причин «омоложения» данного вида преступности является популярность среди молодежи многочисленных социальных сетей и игр, которые стали неотъемлемой частью досуга молодежи. Самой популярной сетевой платформой признается «ВКонтакте» (13 млн авторов, т.е. 10% граждан нашего государства), второй по популярности социальной сетью является Twitter, за ним по популярности следует YouTube [7]. В данных ресурсах экстремистские организации проводят пропагандистско-агитационную и вербовочную деятельность, направленную на увеличение числа сторонников радикальных идей, используют в своих целях несформировавшееся молодежное сознание. Важно, что для совершения данных преступлений необходимо иметь компьютер и быть подключенным к сети Интернет.

13 апреля 2018 года в Таганском суде г. Москвы было вынесено решение о блокировке мессенджера Telegram на территории России. Роскомнадзор совместно с ФСБ России выступил с ходатайством о его блокировке [8]. Telegram представлял собой «секретный чат», который дает возможности приватного общения, такие как шифрование трафика на устройствах, запрет пересылки сообщений, возможность удаления переписки на обоих телефонах, наличие таймера самоуничтожения сообщений и др. Данный контент не был заблокирован, а утратил лишь часть своих функциональных возможностей.

Также в сети Интернет с целью вовлечения молодежи в экстремистскую и террористическую деятельность внедряются многоэтапные электронные игры. В процессе игры подключаются не только зрительные и слуховые, но и тактильные ощущения, тем самым создается практически полный эффект физического присутствия. Особую опасность представляют игры, в которых необходимо выполнять виртуальные задания в реальной жизни. Так, экстремистским сообществом «Северное братство» была разработана компьютерная онлайн-игра «Большая игра. Сломай систему». Главной целью этого проекта было увеличение числа участников для дальнейшего проведения ими диверсий против основ конституционного строя Российской Федерации. Игра была устроена в форме структурированного взаимодействия, где все игроки разделялись на различные уровни («уличный боец», «интернет-боец») и каждый имел свои конкретные задачи по сбору информации и выполнению конкретных действий [9. — С. 10]. Данный интернет-проект в 2011 году был признан экстремистским.

В. С. Соловьевым было проведено исследование, в ходе которого проанализированы 300 обвинительных приговоров, вынесенных с 2008 по 2014 год судами первой инстанции. Все анализируемые преступления совершались исключительно в социальных сетях. На основании полученных данных можно сделать следующие выводы: чаще всего объектами экстремистских проявлений выступают представители Северного Кавказа еврейского народа (16,30%), выходцы из Средней Азии и русские составляют (11,60%), в приговорах также фигурируют и представители других народов. В основе своей информация экстремистской направленности представлена в виде: видеофрагментов (51,2%); текста (30,8%); графических изображений (10,3%); на последнем месте сведения представленные в виде аудиофайлов (7,7%) [10. — С. 65].

Для противодействия экстремистской деятельности и разработки предупредительных мер в сфере субъектно-объектных отношений необходимо решить ряд правовых и организационных вопросов, в том числе касающихся анонимности и защищенности от перехвата передаваемой по сети информации. Радикально настроенные граждане для распространения агитационной информации используют ресурсы, не требующие регистрационных действий (авторизации), подмену IP-адреса посредством перенаправления запросов на удаленные серверы, которые могут находиться в разных государствах, что создает определённые затруднения в деятельности правоохранительных органов. Например, в США были разработаны протоколы и технологии в информационной сети Интернет, а корпорация по управлению доменными именами и IP-адресами была создана совместно с американским правительством и находится на территории данного государства. Наиболее используемые мировые сетевые серверы (Google, Microsoft, поисковая система Bing, система телефонии Skype, Facebook) свои вычислительные мощности, а также руководящий и обслуживающий персонал сосредоточили на территории США. Соответственно, сведения о пользователях перечисленных систем находятся в распоряжении американских компаний и спецслужб [11. — С. 110].

Одним из действенных рычагов в противодействии экстремизму являются мониторинг и своевременная блокировка интернет-ресурсов, содержащих противоправную информацию. В соответствии со ст. 13 Федерального закона РФ от 25 июля 2002 г. «О противодействии экстремистской деятельности» [12], п. 7 Положения о Министерстве юстиции Российской Федерации данную

деятельность на территории Российской Федерации, а именно ведение, опубликование и размещение в сети Интернет федерального списка экстремистских материалов, осуществляет Министерство юстиции Российской Федерации. На официальном сайте Минюста России опубликован список из более 4000 материалов [13]. МВД России совместно с ФСБ России и Роскомнадзором в 2018 году начало применять обновленные системы по поиску и выявлению копий сайтов, которые идентичны ранее заблокированным.

Если данная разновидность преступности носит настолько глобальный характер, необходимо создать единый орган, главной задачей которого будет мониторинг интернет-пространства. В настоящее время в Российской Федерации существует система государственных учреждений и организаций, осуществляющих работу по противодействию экстремизму, на основе деятельности которой можно выделить следующие направления борьбы с этим негативным явлением: совершенствование законодательства; координация ОВД как на территории Российской Федерации, так и за ее пределами в рамках антитеррористической деятельности; создание ФСБ и МВД России специализированных служб, осуществляющих борьбу с терроризмом; формирование единых информационной и прогностической систем учета и регистрации; оперативно-профилактическая и пропагандистская работа ОВД и специальных служб. Однако деятельность данных органов по взаимодействию не отрегулирована.

В частности, С. Н. Миронов, И. М. Усманов и другие авторы считают, что для успешного противодействия экстремизму необходимо не только сотрудничество ведомств, служб и специальных подразделений, но и участие в данной деятельности бдительных интернет-пользователей [14. — С. 13].

Необходимо скорректировать и унифицировать статистическую форму отчетности ГИАЦ МВД России. Не в полной мере используется потенциал статистической отчетности соответствующими службами и подразделениями, занимающимися выявлением причин и условий совершения преступлений, определением закономерностей их совершения, с последующей разработкой механизма предупреждения преступлений, совершаемых в исследуемой сфере.

В этих целях необходимо проводить социальный мониторинг среди населения, направленный на борьбу с радикально настроенными гражданами в виртуальных сообществах. При этом бесконтрольность приведет к снижению эффективности деятельности органов государственной власти, в том числе и органов внутренних дел. Проявления экстремизма в дальнейшем могут перерасти в межэтноконфессиональные противоречия и,

как следствие, в преступления, совершаемые на этой почве.

ЛИТЕРАТУРА

1. Данные Фонда общественного мнения // Официальный сайт. — URL: <http://fom.ru/SMI-internet/13585> (дата обращения: 15.02.2019).
2. Данные Генеральной прокуратуры РФ // Официальный сайт. — URL: <http://www.genproc.gov.ru/> (дата обращения: 12.04.2019).
3. Шакирьянов М. М. Пути повышения эффективности расследования преступлений экстремистской направленности в сети // Вестник Казанского юридического института МВД России. — 2018. — № 4 (34). — С. 549—555.
4. Петрянин А. В. Уголовно-правовые, оперативно-разыскные и криминалистические механизмы противодействия экстремизму в телекоммуникационных сетях и сети Интернет: на примере статьи 280 УК РФ // Вестник Нижегородской академии МВД России. — 2016. — № 1 (13). — С. 158—161.
5. Данные Минюста РФ // Официальный сайт. — URL: https://minjust.ru/nko/perechen_zapret (дата обращения: 12.04.2019).
6. Демидова-Петрова Е. В. Криминогенность несовершеннолетних сквозь призму криминологически значимых проявлений экстремизма // Ученые записки университета. — 2018. — Т. 160, кн. 2. — С. 476—486.
7. Данные Аналитического центра // Официальный сайт. — URL: <https://branalytics.ru/statistics/author> (дата обращения: 15.12.2018).
8. Данные «Российской газеты» // Официальный сайт. — URL: <https://rg.ru/2018/04/13/sud-vynes-reshenie-o-blokirovke-telegram.html> (дата обращения: 15.12.2018).
9. Кочубей М. А. Профилактика терроризма и экстремизма в молодежной среде. — СПб : Русь, 2018. — 96 с.
10. Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10, № 1. — С. 60—72.
11. Стукалов В. В., Запорожец Е. В. Проблемы противодействия экстремизму в сети Интернет // Общество и право. — 2016. — № 4 (58). — С. 108—112.
12. О противодействии экстремистской деятельности : федеральный закон от 25 июля 2002 г. № 114-ФЗ [Электронный ресурс] // СПС «Консультант-Плюс». — URL: http://www.consultant.ru/document/cons_doc
13. Данные Минюста РФ // Официальный сайт. — URL: <https://minjust.ru/ru/node/243787>
14. Миронов С. Н., Абдулганеев Р. Р., Артюшина О. В. Противодействие органов внутренних дел экстремизму и терроризму : учебное пособие. — Казань, 2017. — 175 с.
15. Фадеев В. Н., Мезенцев С. А. Нарушение суверенитета России — криминологическая проблема // Вестник экономической безопасности. — 2018. — № 1. — С. 184—197; — № 2. — С. 40—54; — № 3. — С. 54—67.

