Владимир Олегович Давыдов,
доктор юридических наук, доцент,
почетный сотрудник МВД России,
лауреат премии МВД России в области науки,
профессор кафедры правосудия
и правоохранительной деятельности
Тульский государственный университет
E-mail: VladDv71@yandex.ru

О некоторых аспектах практики реализации криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве

Аннотация

Рассматриваются общетеоретические и практические аспекты криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве. Автором на основе изучения современных научных подходов и анализа результатов практики противодействия преступлениям исследуемого рода отстаивается позиция о признании криминалистического предупреждения одним их приоритетных направлений деятельности правоохранительных органов в противодействии экстремизму, что способствует своевременному выявлению и минимизации причин и условий данного вида противоправной деятельности.

Ключевые слова и словосочетания: *криминалистическое предупреждение; преступления экстремистской направленности; экстремизм; информационно-телекоммуникационное пространство; криминалистически значимая информация; цифровые следы; мониторинг; контент.*

Перемены начала XXI столетия, связанные с научно-техническим прогрессом в области цифровой коммуникации, в той или иной мере сказались на всех сферах жизни мирового социума и привели к беспрецедентному расширению возможностей доступа к самому разнообразному спектру информационных ресурсов. Новейшие цифровые технологии способствовали дальнейшему «сжатию» пространства и времени, обусловили усиление социальной активности индивидов и, бесспорно, послужили созидатель-

ным целям повышения эффективности общественных и государственных институтов.

Однако еще в эпоху XIX столетия великий русский мыслитель Л. Н. Толстой отмечал, что повсеместно «прогресс одной стороны человеческой жизни выступает регрессом другой ее стороны» [5]. Так и обозначенные нами инновации, в значительной степени, функционирующие независимо от государственного контроля и не поддающиеся в полной мере политическому контролю со стороны государственных институтов, детерминировали тенденцию достаточно устойчивой причинно-следственной связи между количественным разнообразием цифровых технологий коммуникации, с одной стороны, и качественными изменениями механизма преступной деятельности экстремистской направленности с другой.

В этой связи обратим внимание на два достаточно интересных в аспекте исследуемой проблематики факта. В конце 90-х гг. прошлого столетия американский эксперт Уэйн Раш, специализирующийся на проблемах в сфере информационно-телекоммуникационных технологий, прогнозировал, что «в недалеком будущем радикальные группы полностью адаптируются к использованию сети Интернет как инструмента коммуникации, организации, вербовки, сбора денежных средств, стратегического позиционирования, связи с медиа» [6]. Несколько позднее, профессор коммуникаций университета г. Хайфе (Израиль) Габриэль Вайман, начавший отслеживать и изучать террористические web-сайты еще с середины 1990-х годов, в научной работе «Террор в Интернете: новая арена битвы, новые вызовы», указывал уже на восемь типовых направлений, по которым террористы реализуют свои цели в сети Интернет. А именно: проведение психологической войны; поиск информации; обучение; сбор денежных средств; пропаганда; вербовка; организация сетей; планирование и координация действий [7].

Не вдаваясь в дальнейшую полемику по поводу научных публикаций, полагаем возможным сделать следующий вывод: в современных условиях способы цифровой коммуникации стали одним из узловых элементов в механизме преступной деятельности экстремистской направленности. Актуальность данного тезиса наглядно подтверждается данными официальной статистики ГИАЦ МВД России: за 11 мес. 2022 г. на территории Российской Федерации было зарегистрировано 1 407 (+43,1 %) преступлений экстремистской направленности, из которых 473 (+80,0 %) преступных деяния, предусмотренные ст. 280 Уголовного кодекса Россий-

ской Федерации, были совершены с использованием информационно-телекоммуникационных технологий [4].

Очевидно, что данному обстоятельству в немалой степени способствуют закономерности двойственной социально-технологической природы информационно-телекоммуникационного пространства, а также наличие у подобных цифровых технологий определенного криминально привлекательного функционала. В числе последнего выделим такие значимые элементы, как:

– потенциальная возможность осуществления анонимного доступа к информационно-телекоммуникационной среде и, как следствие, к масштабной аудитории ее пользователей;

– дистанционность субъекта совершения преступных действий экстремистской направленности, как от информационного продукта, так и от места наступления негативных последствий этих действий;

– высокая скорость распространения информационного контента и мультимедийность среды коммуникации;

– непостоянство и динамичность изменения информационных объектов;

– распределенность информационных баз и возможность управления ими различными субъектами посредством предоставления прав доступа;

– недостаточная эффективность существующих механизмов государственных цензуры и контроля;

– постоянно возрастающий технологический потенциал, позволяющий, в числе прочего, дистанционно координировать действия менее четко организованных структур радикальной направленности, а также отдельных лиц, намеренных осуществлять экстремистские действия децентрализованно и др.

Таким образом, информационно-телекоммуникационное пространство в современных условиях закономерно выступает значимым объектом криминалистического предупреждения преступлений экстремистской направленности как неотъемлемая часть системы общественных отношений, содержащей криминалистически значимую компьютерную информацию о подготавливаемых, совершаемых и уже совершенных преступных деяниях подобного рода.

Само же криминалистическое предупреждение преступлений экстремистской направленности в информационно-телекоммуникационном пространстве, на наш взгляд, следует рассматривать как деятельность, основанную на специальных средствах, приемах и методах науки криминалистики, направленную на выявление,

собирание, исследование и использование криминалистически значимой компьютерной информации об обстоятельствах, способствующих подготовке, совершению и сокрытию таких преступных деяний (а в ряде случаев, намеренному афишированию преступного результата), на устранение указанных обстоятельств, а также на предупреждение готовящихся и пресечение начавшихся преступлений.

Полагаем, что складывающаяся в настоящее время ситуация настоятельно требует своего дальнейшего научного осмысления в интересах своевременного выявления, действенного пресечения и эффективного предупреждения преступлений рассматриваемого рода.

Так, например, в аспекте решения современных задач криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве значимым будет являться такое уже названное нами «криминальное» свойство, как удаленность субъекта совершения преступных действий от информационного продукта и от места наступления негативных последствий этих действий. Например, действия, направленные на склонение, вербовку и иное вовлечение лица в преступную деятельность экстремистского формирования, совершенные с использованием глобальной сети Интернет, достаточно часто осуществляются в одном географическом регионе, а ее негативные последствия, т. е. непосредственное вступление индивида в региональную экстремистскую группу «сетевого» организационного модуля, наступают в другом [2].

При этом значительные трудности в выявлении криминалистически значимой компьютерной информации о причастности организаторов, посредников и исполнителей к преступной деятельности рассматриваемого рода будут связаны с обнаружением цифровых следов информационного объекта в сетевых ресурсах информационно-телекоммуникационного пространства.

В этой связи представляется обоснованной научная позиция А.М. Багмета, В.В. Бычкова, С.Ю. Скобелина и Н.Н. Ильина, согласно которой под понятием «цифровой след» надлежит понимать любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [1].

К числу основных объективных форм существования криминалистически значимой компьютерной информации в аспекте криминалистического предупреждения преступных деяний экс-

тремистской направленности в информационно-телекоммуникационном пространстве следует отнести: сетевой адрес, доменное имя, web-сайт и страницу web-сайта. В целях выявления цифровых следов данного характера видится целесообразным рекомендовать использование сервисов, функционал которых позволяет получать следующие категории сведений: о датах регистрации домена и окончания периода его преимущественного продления; о регистраторе, осуществляющем поддержку доменного имени; об администраторе домена (однако только в том случае, если администратор не воспользовался услугой сокрытия персональных данных). В числе данных сервисов следует выделить, например: *www.ripn.net/nic/whois/, www.reg.ru/whois/, www.nic.ru/whois/, www.2ip.ru/whois/* и др.

Предполагается, что надлежит придавать значение и тому факту, что функционал дистанционной коммуникации привел к определенной трансформации самой структуры организационного построения преступных формирований экстремистской направленности (в т. ч. носящих транснациональный характер). В настоящее время в «сетевом» модуле все большее распространение получают группы с преобладанием так называемых «горизонтальных» преступных связей, основанных не столько на строгом подчинении «иерархическому» модулю экстремистского формирования, а сколько на общих региональных криминальной цели и мотивации радикальной деятельности [3].

С учетом данной тенденции, при поиске криминалистически значимой компьютерной информации в информационно-телекоммуникационном пространстве, наряду с учетом особенностей совершения преступлений экстремистской направленности с использованием средств дистанционной коммуникации, следует иметь ввиду, во-первых, естественно возникающие условия, характеризующиеся тем, что, хотя действия и контакты пользователей достаточно часто анонимны, но при этом они остаются публичными, а во-вторых, специфику среды обращения информации в сетях, т. е. формы коммуникации, принятые в радикальной «электронной» среде.

Технологически ведение поиска криминалистически значимой информации о преступной деятельности экстремистской направленности в информационно-телекоммуникационном пространстве следует осуществлять с использованием запросов на специализированном языке (характерный сленг (фразы, словосочетания), названия экстремистских материалов и т. п.), а также учитывая особенности психологии потенциальных «партнеров» по общению (их внушаемость, конформизм, склонность к соперничеству, предпочитаемые интернет-ресурсы, статус в интернет-сообществах и т. п.).

В частности, необходимые лексические единицы могут подбираться посредством использования сведений, размещаемых в Федеральном списке экстремистских материалов на официальном сайте Министерства юстиции Российской Федерации[1].

Безусловно, к проведению поиска рационально привлекать как лиц, обладающих специальными техническими познаниями в сфере цифровых технологий, так и специалистов-лингвистов, компетентных отождествить уголовно наказуемые признаки преступлений экстремисткой направленности. Реализация подобных мер позволит обеспечить своевременное выявление криминалистически значимой компьютерной информации о признаках подготовки и планирования экстремистских акций, вербовочных действий, сбора финансовых средств и других форм ресурсного обеспечения экстремистской деятельности.

Еще одним из направлений поиска криминалистически значимой компьютерной информации в информационно-телекоммуникационном пространстве должен являться мониторинг по заданным реквизитам интернет-ресурсов, на которых имеются сведения об экстремистской деятельности. Однако наблюдать за всеми web-ресурсами глобальной сети Интернет либо ее российского сегмента Рунет, безусловно, не представляется возможным ввиду их громадного количества. В этой связи наиболее доступный мониторинг информационных ресурсов должен реализовываться посредством русскоязычных поисковых систем (например, Yandex, Google, Mail.ru, Rambler, Bing и других), использующих индексирование всего содержания максимально возможного числа web-страниц и позволяющих производить мониторинг как в отдельных элементах внутри самой web-страницы, так и в связанной с ней информации, а также в относящихся к ней служебных данных (например, внутри заданного домена, типа документа и т. п.). Поиск возможно вести по самим хостам и по словам, находящимся на заданных web-страницах.

Акцентируем внимание на том факте, что, помимо уже названных систем поиска, существуют и специализированные интеллектуальные метапоисковые системы (например, AskNet, Excite, Ixquick или известный совместный проект Московского государственного университета имени М. В. Ломоносова и Стэнфордского университета «Нигма.РФ»), осуществляющие формирование поисковой выдачи и кластеризацию информации за счет смешивания результатов поиска по общедоступным базам иных систем

[1] URL: https://minjust.gov.ru/ru/extremist-materials/.

(например, Google, Yahoo, Bing», Yandex, Rambler, AltaVista, Aport и др.).

Как следствие, осуществление содержательного анализа сетевых информационных объектов в виде видео-, аудио- и текстовых форм с применением специализированного программного софта позволяет своевременно выявлять наличие признаков сведений, представляющих потенциальный интерес в аспекте решения задач криминалистического предупреждения экстремистской деятельности и в т. ч. признаков подготовки вербовочных акций в объектах, содержащих зашифрованные и иносказательные фразы, отдельные слова, графические файлы и т. п.

Нередко в ходе поисковых мероприятий в открытых источниках информационно-телекоммуникационного пространства встречаются ссылки на закрытые web-ресурсы, на которых наряду с популяризацией идеологии экстремизма осуществляется также деятельность, направленная на склонение, вербовку и иное вовлечение лиц в преступную деятельность экстремистской направленности. Содержание работы по поиску криминалистически значимой компьютерной информации на подобных web-ресурсах должно включать всестороннее изучение его контента, проведение проверки его расположения на технических площадках хостинг-провайдера, установление данных регистранта, а также сведений об авторе «проекта» и его активных участниках.

Очевидно, что определить всю совокупность направлений криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве и создать тем самым их систему закрытого типа практически невозможно по причине динамичного развития цифровых средств коммуникации. Данное обстоятельство даже в обозримой перспективе не позволяет предусмотреть все возможные варианты появления и развития причин и условий, которые могут способствовать совершению преступных деяний рассматриваемого рода.

Полагаем, что разрешение задач криминалистического предупреждения преступлений экстремистской направленности в информационно-телекоммуникационном пространстве представляет собой комплексное предупредительное воздействие, эффективность которого в значительной степени будет основана на том факте, что сотрудник правоохранительного органа должен быть вооружен научно обоснованным знанием о нем в самом широком смысле этого понятия – от его природы и содержания до частных причин и условий, способствующих преступлению.

Список литературы:

1. *Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н.* Цифровые следы преступлений : моногр. М., 2021.

2. *Давыдов В. О.* Методика расследования транснациональной преступной деятельности экстремистского характера : дис. ... д-ра юрид. наук. Ростов-на-Дону, 2019.

3. *Давыдов В. О.* Научные основы базовой методики расследования преступлений и их развитие в практике борьбы с транснациональным экстремизмом : моногр. М., 2020.

4. Состояние преступности в России (за январь–ноябрь 2022 года). М., 2022.

5. *Толстой Л. Н.* Полное собрание сочинений : в 90 т. : Педагогические статьи (1860–1863 гг.). М., 1936. Т. 8.

6. *Rash W.* Politic on the nets: Wiring the political process. New York, 1997.

7. *Weimann G.* Terror on the Internet: The New Arena. Washington, DC, 2006.