

НЕКОТОРЫЕ ВОПРОСЫ УСТАНОВЛЕНИЯ СПОСОБОВ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СЕТИ ИНТЕРНЕТ

В настоящей статье рассматриваются специфические способы совершения противоправных деяний радикального характера, совершаемые при помощи информационно-телекоммуникационных технологий. Способ подготовки, совершения и сокрытия преступлений экстремистской направленности является не только элементом криминалистической характеристики экстремизма в теоретическом отношении, но и имеет важное практическое значение. Во-первых, для целей выявления преступлений и закрепления следов в информационном пространстве, а во-вторых, для доказывания цели, мотивов, события преступления и других обстоятельств, установленных уголовно-процессуальным законом. Выявленные особенности преступлений, совершаемых при помощи сети Интернет, позволяют реализовывать в должной мере задачи правоохранительных органов в борьбе с экстремизмом в России.

Ключевые слова: способ преступления, экстремизм, коммуникация, социальные сети, кибертерроризм.

V.S. Kryazhev

SOME ISSUES OF ESTABLISHING METHODS OF EXTREMIST CRIMES ON THE INTERNET

This article examines the specific ways of committing illegal acts of a radical nature committed with the help of information and telecommunication technologies. The method of preparation, commission and concealment of extremist crimes is not only an element of the criminalistic characteristics of extremism in theory, but also has important practical significance. Firstly, for the purpose of detecting crimes and fixing traces in the information space, and secondly, to prove the purpose, motives, events of the crime and other circumstances established by the criminal procedure law. The identified features of crimes committed using the Internet make it possible

to adequately implement the tasks of law enforcement agencies in the fight against extremism in Russia.

Keywords: the method of crime, extremism, communication, social networks, cyberterrorism.

Следует признать, что всемирная паутина – информационно-телекоммуникационная сеть Интернет является не только бесспорным достижением современности, но и воплощением многих известных пороков общества, в недрах которого уже создаются новые виды и формы преступной деятельности. В контексте обозначенной темы это и прежде всего распространение информации, связанной с экстремистской идеологией, создание сообществ радикально настроенных лиц с целью совершения противоправных деяний, распределение между ними зон влияния, ролей, осуществление коммуникации и прочее. Интернет также является мощным средством идеологической поддержки и информационного воздействия со стороны деструктивных экстремистских организаций, например международных террористов и бандитских формирований экстремистской направленности. Интернет используется для создания баз разведывательных данных, перехвата информации правоохранительных органов, вербовки сообщников, сбора пожертвований, размещения руководств по организации терактов, психологического терроризма, сбора информации о предполагаемых целях и объектах шантажа, подготовки террористов, пропаганды расовой, религиозной и других форм нетерпимости. В последнее десятилетие получил распространение так называемый электронный «джихад», или кибертерроризм [1, с. 24–25].

Правоохранительные органы ведут борьбу с распространением информации подобного толка, принимают меры по выявлению сайтов, содержащих информацию о способах изготовления взрывных устройств, осуществления террористических актов, а также сайтов, содержащих экстремистские материалы, и т.п. Однако наряду с достижением положительных результатов приходится сталкиваться со множеством проблем. Так, введенное ограничение доступа пользователей к конкретным сайтам не гарантирует того, что его информационные материалы не появят-

ся на других ресурсах с несколько видоизмененным названием в адресе сайта [2, с. 5].

Необходимо учитывать и роль социальных сетей, посредством ресурсов которых осуществляется передача информации через так называемые сообщества или группы пользователей той или иной социальной сети. Эта информация распространяется очень быстро в силу того, что многие пользователи сети Интернет постоянно находятся в режиме онлайн через мобильные устройства [3, с. 67]. Они передают в сети различную информацию, фотографии, видеоматериалы, копируют ссылки на адреса сайтов, оставляют комментарии и т. п. Наиболее распространенными социальными сетями и мессенджерами в настоящее время являются: «Одноклассники», «VK», «WhatsApp», «Viber», «Telegram», «TikTok», «Facebook» и «Instagram»¹ и некоторые другие.

В этом контексте необходимо отметить, что вышеуказанные социальные сети значительно упрощают поиск лиц, наиболее легко подверженных влиянию и радикализации. Платформы социальных сетей полны групп людей, ищущих помощи и поддержки, и желающие воспользоваться этим могут легко присоединиться к этим группам, войти в контакт и даже подружиться с так называемым уязвимым человеком. При этом манипулятивное воздействие на психику оказывается лидерами и членами преступных объединений с привлечением достаточно широкого арсенала. Ими используются самые различные средства, как самые простые – откровенно фейковые сообщения, так и более сложные технологии – геймификация; фрейминг; методы рекламы и маркетинга, в частности методика Монро, широко используемая при создании текстов для мотивационных выступлений.

В обозначенных случаях Интернет является исключительно инструментом, с помощью которого оказывается воздействие на сознание людей при установлении диалоговых отношений в общении. Сама информационно-телекоммуникационная сеть не является движущим причинным фактором радикализации.

Однако, несмотря на это, Интернет обладает функциями и механизмами, поддерживающими процессы распространения и

¹ Facebook и Instagram – запрещенные в Российской Федерации, так как базируются на признанной судом Российской Федерации экстремистской платформе Meta.

пропаганды экстремистской идеологии, а также усиливающими воздействие соответствующей информации на сознание пользователей сети. В данном случае речь идет о том, каким образом в Интернете отбирается, связывается и обрабатывается информация как в силу архитектуры самой сети, так и посредством действий ее пользователей. Яркий пример: формирование эхо-камер и пузыря фильтров (пузыря алгоритмов), в которых пользователи оказываются в полной изоляции от иных альтернативных взглядов, ценностей и ориентиров. Так, большинство социальных сетей и поисковых систем работают по алгоритму, который самостоятельно подбирает контент на основе предпочтений (лайки и дизлайки) пользователей и информационных запросов соответственно. Недостаток этого алгоритма в том, что искусственный интеллект окружает конкретного пользователя «голосами» других пользователей, придерживающихся аналогичной с ним точки зрения. Тем самым происходят усиление индивидуальной системы убеждений пользователя и одновременное искажение общей картины действительности. Таким образом, создается эхо-камера, которая не пропускает альтернативной точки зрения, и, соответственно, у пользователя дополнительно усиливается уверенность в правильности занимаемой им позиции [4, с. 458–459].

Обнаружить экстремистские и террористические материалы в «сообществах и группах» социальных сетей и мессенджеров довольно сложно, а ограничить к ним допуск пользователей практически невозможно. Однако вместе с тем в ходе расследования преступлений сотрудники правоохранительных органов имеют возможность использовать информацию из социальной сети по отдельным пользователям для установления их связей, контактов и отчасти по передаваемой ими информации, если аккаунт пользователя не скрыт настройками приватности или не заблокирован для посторонних пользователей.

Способ совершения преступления проявляется чаще всего в активных действиях преступников. Способы совершения преступлений экстремистской направленности отличаются многообразием и ставятся в зависимость от конкретных обстоятельств. Тем не менее общее, что объединяет все способы совершения преступлений экстремистской направленности, – возбуждение

расовой, национальной, этнической, религиозной ненависти или иной вражды по отношению к другим социальным группам, их представителям, а также распространение этих идей в массы.

Необходимо отметить, что, совершая преступления экстремистского характера преступники преследуют и цель расширения круга своих сторонников. Так, при совершении преступных деяний, помимо распространения информации экстремистского характера, происходит воздействие на сознание и волю людей, что предопределяет их поведение в дальнейшем (к примеру, может подтолкнуть к объединению и созданию новых преступных формирований на этой почве).

Совершая те или иные противоправные действия информационного характера, причастные к экстремистской деятельности лица, понимают уголовно-правовую значимость последствий. В силу этого ими предпринимаются определенные действия по сокрытию преступлений. Изъятие информации из сети Интернет осуществляется разными способами.

1. Сокрытие путем уничтожения информационных следов, которые потенциально могут служить доказательствами совершения преступления. Как правило, уничтожаются не только посты и аккаунты, относящиеся напрямую к событию преступления, но и потенциально опасные с точки зрения информативности объекты (фотографии, видеоролики, история браузера и т.д.).

2. Сокрытие посредством утаивания информации и ее источников (электронные устройства и накопители информации). Кроме того, сокрытие информации о преступлении может осуществляться посредством кодирования электронных устройств.

3. Сокрытие преступления путем маскировки. Как правило маскировка предполагается на стадии подготовки к совершению преступного деяния. Например, форма публичного выступления может реализовываться в общеизвестном месте конкретным исполнителем, при этом маскируется внешность (маски, балаклавы, шарфы и капюшоны), транспортные средства (скрываются государственные регистрационные знаки автомобиля). При совершении данной категории преступлений в сети Интернет экстремисты стремятся использовать прозвища, которые нередко совпадают с именами реальных исторических личностей или

лиц, придерживающихся экстремистских взглядов. К элементам маскировки также необходимо относить и конкретные действия экстремистов: использование шифрования при отправке сообщений на электронную почту по специально созданным электронным адресам, а также специальных программ в сети Интернет.

Совершение преступлений экстремистской направленности отличается многообразием способов и сложностью действий. В большинстве случаев исследуемая категория преступлений тщательно планируется и готовится, что предполагает поэтапное применение масштабного арсенала способов совершения деяний, среди которых в настоящее время особую актуальность приобретают действия, реализуемые посредством сети Интернет. Кроме того, большое значение для расследования данных преступлений приобретает оценка способов сокрытия преступного деяния – не только следов его совершения, но и средств и орудий, а также предметов, так или иначе способных стать доказательством по делу.

Таким образом, при расследовании преступлений экстремистской направленности, необходимо ориентироваться не только на цели и мотивы совершения деликтов, но и исследовать способ преступления. Традиционно в криминалистике способ преступления (подготовка – совершение – сокрытие) является важным элементом в установлении корреляции с другими элементами криминалистической характеристики преступлений экстремистской направленности. Рассматриваемые деяния включаются в эту трехэлементную составляющую криминалистической характеристики экстремизма и находят свое отражение в цифровом пространстве. Исследуя социальные сети, аккаунты пользователей и некоторые иные информационные ресурсы сотрудники правоохранительных органов должны выявлять закономерные связи информации, содержащейся на том или ином информационном портале с деятельностью конкретных лиц, причастных к незаконной деятельности с целью дальнейшего ее пресечения и доказывания.

Список использованной литературы

1. Полякова Т.А. Вопросы ответственности за использование информационно-телекоммуникационных систем в террори-

стических и экстремистских целях / Т. А. Полякова // Российский следователь. – 2008. – № 1. – С. 24–27.

2. Денисов Ю.Д. Противодействие экстремизму в сети Интернет / Ю.Д. Денисов // Законность. – 2009. – № 6. – С. 3–5.

3. Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет / А.Г. Куликов // Криминалистика: вчера, сегодня, завтра. – 2021. – № 2. – С. 64–71.

4. Бешукова З.М. Влияние информации в сети «Интернет» и социальных сетях на формирование экстремистских и террористических взглядов в молодежной среде / З.М. Бешукова // Личность преступника в изменяющемся мире (Долговские чтения) : материалы 3-й Всерос. науч.-практ. конф. (Москва, 23–24 марта 2023 г.) / науч. ред. В.В. Меркурьев, Ю.А. Тимошенко ; Ун-т прокуратуры Рос. Федерации, Рос. криминолог. ассоц. – М., 2023. – С. 456–461.

Информация об авторе

Кряжев Владимир Сергеевич – кандидат юридических наук, доцент, кафедра криминалистики, судебных экспертиз и юридической психологии, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: kryagevvs@mail.ru.

Author

Kryazhev Vladimir Sergeevich – Candidate of Law, Associate Professor, Department of Criminology, Forensic Examinations and Legal Psychology, Baikal State University, Irkutsk, the Russian Federation, e-mail: kryagevvs@mail.ru.