

DOI 10.46741/2686-9764-2020-14-3-388-393

УДК 343.985

## **Особенности использования сети Интернет в расследовании преступлений экстремистской направленности**

**Н. И. ГЕРАСИМЕНКО**

Омская академия МВД России, г. Омск, Российская Федерация

ORCID: <https://orcid.org/0000-0002-1107-5337>, e-mail: [ninella007@mail.ru](mailto:ninella007@mail.ru)

**Р е ф е р а т:** Достаточно большое количество преступных деяний можно отнести к преступлениям экстремистской направленности, но не все из них можно совершать посредством Интернета. Такого рода преступления имеют ряд характерных особенностей, которые подлежат установлению на первоначальном и последующих этапах расследования: 1) обстановка совершения преступлений, включающая место и время (возможность совершения преступления лицом, находящимся в любой точке земного шара, где есть доступ в Интернет; преступление может совершаться длительное время – с момента размещения информации экстремистской направленности в сети до момента ее блокировки); 2) способы совершения преступлений (размещение информации, содержащей элементы экстремистского характера (тексты, картинки, посты, песни и т. п.), большие возможности для сокрытия преступного действия). Помимо шифрования файлов существует возможность их быстрого удаления с информационных носителей. Учитывая эти обстоятельства, первоочередными являются незамедлительное фиксирование информации с экстремист-

ской направленностью, содержащейся на электронных носителях, и выявление лиц, ее разместивших. При этом ключевыми моментами в расследовании должны стать проведение осмотра интернет-ресурса с обязательным указанием электронного адреса, наименования, сведений об обратной связи, контактах, а также назначение компьютерной и лингвистической экспертиз.

Ключевые слова: экстремистская деятельность; осмотр; сеть Интернет; способ; удаленный файл; сокрытие информации.

12.00.12 – Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность.

Для цитирования: Герасименко Н. И. Особенности использования сети Интернет в расследовании преступлений экстремистской направленности. *Пенитенциарная наука*. 2020; 14(3):388–393. DOI 10.46741/2686-9764-2020-14-3-388-393.

## Specifics of using the Internet in the investigation of extremist crimes

### N. I. GERASIMENKO

Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk, Russian Federation

ORCID: <https://orcid.org/0000-0002-1107-5337>, e-mail: [ninella007@mail.ru](mailto:ninella007@mail.ru)

**Abstract:** A fairly large number of criminal acts can be attributed to crimes of an extremist nature, but not all of them can be committed via the Internet. This type of crime has a number of characteristic features that must be established at the initial and subsequent stages of the investigation: 1) the situation in which the crimes were committed, including place and time. A feature of the place is the possibility of committing a crime by a person located anywhere in the world where there is Internet access. The specifics of time include the fact that a crime can be committed for a long time – from the moment extremist information is posted on the network until it is blocked; 2) the methods of committing the considered category of crimes, the features of which are the placement of information containing elements of an extremist nature (texts, pictures, posts, songs, etc.), as well as great opportunities for concealing the crime. In addition to encrypting files, it is possible to quickly delete them from information carriers. Given these circumstances, the priority is the immediate recording of information with an extremist orientation contained in electronic media, and the identification of the persons who posted it. At the same time the key points in the investigation should be the examination of the Internet resource with the obligatory indication of the email address, name, information about feedback, contacts, as well as the appointment of computer and linguistic expertise.

**Key words:** extremist activity; inspection; Internet; means; deleted files; hiding information.

12.00.12 – Forensics; forensic activity; operational investigation.

For citation: Gerasimenko N. I. Specifics of using the Internet in the investigation of extremist crimes. *Penitenciarная наука = Penitentiary Science*. 2020; 14(3):388–393. (In Russ.). DOI 10.46741/2686-9764-2020-14-3-388-393.

В настоящее время массив преступлений, в том числе экстремистской направленности, совершаемых посредством сети Интернет, достаточно велик. Так, по статистическим данным, размещенным на официальном сайте МВД России, с января по декабрь 2018 г. было зарегистрировано 1265 заявлений о совершении преступлений экстремистской направленности, в 2019 г. – 585, с января по март 2020 г. – 210, причем, на наш взгляд, истинные масштабы соответствующей преступной деятельности от-

ражены не в полной мере в силу ее латентности.

Распространенность рассматриваемых противоправных деяний обусловлена, во-первых, удаленностью лица, совершающего преступление, то есть фактической неопределенностью места его нахождения, а во-вторых, снижением уровня оставляемой в результате совершения преступления следовой информации.

Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской

деятельности» не содержит понятия преступлений рассматриваемой категории. В соответствии со ст. 1 данного документа экстремистской деятельностью (экстремизмом) является:

1) деятельность общественных и религиозных объединений, либо иных организаций, либо средств массовой информации, либо физических лиц по подготовке и совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности России, подрыв безопасности страны, захват или присвоение властных полномочий, создание незаконных вооруженных формирований и т. д.;

2) пропаганда и публичное демонстрационное нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения;

3) публичные призывы к осуществлению указанной деятельности или действий;

4) финансирование указанной деятельности либо иное содействие ее осуществлению, в том числе путем предоставления финансовых средств, недвижимости, учебной, полиграфической и материально-технической базы, телефонной, факсимильной и иных видов связи, информационных услуг, иных материально-технических средств.

В соответствии с примечанием 2 к ст. 280 УК РФ под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ.

Проанализировав данное определение, можно заключить, что достаточно много преступлений можно отнести к экстремистским, но не все они совершаются посредством сети Интернет. В данной статье будут рассмотрены ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности), ст. 282 УК РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства), ст. 282.1 УК РФ (организация экстремистского сообщества), ст. 282.2 УК РФ (организация деятельности экстремистской организации).

К преступлениям экстремистской направленности, совершаемым в сети Интернет, содержащимся в иных главах УК РФ, относятся составы ст. 136 (нарушение равенства прав и свобод человека и гражданина), ч. 4

ст. 150 (вовлечение несовершеннолетнего в совершение преступления).

Также к интересующему нас виду можно отнести иные преступления, которые совершены по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы согласно п. «е» ч. 1 ст. 63 УК РФ. Наиболее опасными видами экстремизма являются националистический, религиозный и политический, проявляющиеся в возбуждении ненависти либо вражды по признакам пола, расовой, национальной, языковой, религиозной принадлежности или к какой-либо социальной группе, в том числе путем распространения призывов к насильственным действиям, вовлечения отдельных лиц в деятельность экстремистских организаций или групп, в первую очередь через информационно-телекоммуникационные сети, включая Интернет [4, с. 86].

Размещенная в сети информация зачастую служит поводом для возбуждения уголовного дела, поэтому процессуально грамотная ее фиксация носит принципиальный характер. Нельзя забывать, что сведения могут быть в любой момент удалены преступником – владельцем данной информации.

На основании интервьюирования 80 оперативных сотрудников Центра по противодействию экстремизму УМВД России по Омской области, ГУ МВД России по Новосибирской области, ГУ МВД России по Свердловской области нами были выделены основные проблемы, возникающие при расследовании рассматриваемой категории дел:

1) большое количество пользователей по всему миру;

2) принадлежность сайтов компаниям и пользователям, зарегистрированным за пределами Российской Федерации;

3) распространение информации экстремистской направленности разными способами (песни, текст, видео и др.).

А. С. Бутенко называет следующие причины распространения экстремистских материалов в сети Интернет: 1) многонациональность и многоконфессиональность Российской Федерации, сопровождаемые межнациональной и межрелигиозной напряженностью и высокой конфликтностью общества; 2) экономическая обстановка в стране, в частности социальное расслоение и неприязнь между социальными группами, способствующие быстрому распространению негативного контента в социальных сетях, блогах и чатах; 3) низкий уровень культу-

ры сетевого общения, компенсирующий повышенной эмоциональностью и агрессией [1, с. 60].

Для успешного сбора информации, свидетельствующей о совершении преступления экстремистской направленности, следует обратить внимание на те обстоятельства, которые подлежат установлению на первоначальном и последующем этапах расследования:

1. Обстановка совершения преступления, включающая время и место. Статья 152 УК РФ в ч. 1 определяет место производства предварительного расследования по месту совершения деяния, содержащего признаки преступления. Это значит, что, по общему правилу, местом совершения преступления будет считаться место нахождения лица, распространяющего информацию экстремистского характера. Однако преступления рассматриваемой категории носят транснациональный характер, следовательно, решение о возбуждении уголовного дела может попадать под юрисдикцию той страны, в которой находится лицо, совершающее противоправные действия, и вопрос о возбуждении и дальнейшем расследовании уголовного дела может относиться к компетенции страны, в которой находился преступник в момент совершения им общественно опасного деяния. В данном случае привлечение к уголовной ответственности решается по согласованию между государствами. В связи с этим перед лицом, производящим предварительное расследование, стоит задача не только своевременной фиксации противоправных действий лица, но и скорейшего установления местонахождения преступника для привлечения к уголовной ответственности. Зачастую это невозможно без применения сил и средств оперативных подразделений органов внутренних дел.

Временем совершения преступления признается момент размещения различных сведений экстремистской направленности. Применительно к обстановке совершения преступления следует обратить внимание на ее очевидность, то есть открытость самих действий преступного лица, которое умышленно локализует место либо в силу каких-либо обстоятельств делает его очевидным.

2. Личность совершившего преступление. Согласно статистическим данным МВД России и ФСБ России, более 90 % членов экстремистских организаций – молодые люди в возрасте от 16 до 30 лет. Они и совершают преступления экстремистской направленности. В настоящее время на территории Российской Федерации насчитывается

примерно 150 молодежных экстремистских организаций с четкой устоявшейся идеологией, распределением ролей (иерархией), строгой дисциплиной [5].

В ситуациях, когда преступник не предпринимает никаких действий по своему обезличиванию, например размещает информацию экстремистского характера в учетной записи социальной сети либо вместе с информацией оставляет свои установочные или контактные данные, вопрос об установлении личности остро не стоит. Посредством проведения ряда оперативно-розыскных и иных мероприятий лицо, проводящее предварительное расследование, собственноручно либо путем направления поручения в оперативные подразделения органов внутренних дел определяет преступника, и последующая работа по совершению преступлению облегчается в разы. В случае же когда преступник принимает активные действия по сокрытию сведений о своей личности, комплекс следственных действий и иных проводимых мероприятий существенно расширяется. Наиболее рациональным способом установления личности преступника становится опять же использование сил и средств специальных оперативных подразделений. Говорить о том, что лицо может бесследно разместить сведения экстремистского содержания, не стоит: при любой активности лица в сети остается как минимум IP-адрес, который может служить отправной точкой в определении места совершаемого преступления и установлении личности преступника. Как правило, данная процедура осложняется использованием со стороны преступника различных компьютерных программ, направленных на искажение информации о месте выхода в сеть Интернет, поэтому при направлении поручения в оперативные подразделения органов внутренних дел и получении ответов от них следует в обязательном порядке проводить анализ сведений и вычленять те из них, которые не соответствуют действительности. Помимо прочего, в установлении личности может помочь и создаваемый для совершения преступления ресурс: различные компьютерные программы, скриншоты, интернет-сайты, сообщества. Создаются они в целях достижения скорейшего преступного результата, повышения эффективности преступной деятельности, усиления контроля над запущенными процессами, но в то же время снижают степень обезличенности преступника либо преступного сообщества, ведь введение любого рода инноваций увеличивает количество каналов

обратной связи, то есть преумножает число доказательств причастности того или иного лица к совершаемому преступлению.

Как отмечает О. С. Зубкина, проблема экстремизма имеет особое значение для юга России: ввиду разности культур и обычаев народов Кавказа происходят столкновения на национальной почве, сопровождающиеся созданием экстремистских сайтов, на которых ведутся агрессивные обсуждения [3, с. 54].

3. Способ совершаемого преступления. Если говорить о преступлениях экстремистской направленности, которые совершаются посредством использования сети Интернет, то речь будет идти прежде всего о таком способе совершения преступления, как размещение сведений экстремистской направленности. Информация такого рода может сопровождаться определенными призывами, указаниями как ограниченному, так и неограниченному кругу лиц. Однако не стоит исключительно так понимать рассматриваемое преступление. Зачастую действия экстремистского характера могут совершаться не на просторах Интернета, а в реальной жизни, а всемирная сеть при этом используется как средство коммуникации между членами преступных групп. Существенной разницей между двумя подходами является то, что в первом случае сведения будут носить открытый характер, ведь иначе теряется смысл совершаемого преступления, а во втором – тщательно скрываться. Во многом то, сколько внимания уделяется сокрытию информации о подготавливаемом или совершаемом преступлении, зависит от масштабности последнего. И как уже неоднократно отмечалось, следовательно при обнаружении признаков преступления экстремистской направленности и возникновении сложностей с установлением личности преступника следует обращаться с поручением в оперативные подразделения органов внутренних дел. В тех случаях когда не стоит вопроса о получении скрытой от следователя информации, она фиксируется в общем порядке при проведении следственных действий. Стоит все же подчеркнуть, что такого рода ситуации, когда информация о преступлении будет лежать на поверхности, встречаются крайне редко, ведь сам преступник прекрасно понимает, что это может способствовать установлению его личности правоохранительными органами.

Как уже было сказано, основным способом сокрытия преступления является удаление файлов, свидетельствующих о причастности лица к совершенному престу-

плению. Следует иметь в виду, что удаленные файлы могут быть восстановлены и служить при надлежащем их процессуальном закреплении доказательственной информацией, указывающей на причастность лица к преступлению.

При размещении информации экстремистского характера в сети Интернет, как правило, избираются такие ресурсы, которые обладают, во-первых, большой пропускной способностью, а во-вторых, пониженной степенью цензурности: ВКонтакте, Youtube, Facebook, Instagram, Twitter. Это своего рода информационные платформы, которые позволяют размещать различные сведения вне зависимости от формы их представления.

Для повышения эффективности воздействия размещенной информации и ускорения наступления преступного результата лицами используются различные способы размещения данных: рассылки, видео- и музыкальные материалы, фотографии, стихи, песни на действующих страницах, ссылки на материалы других ресурсов в публикациях и комментариях [2, с. 126].

В качестве базы для совершения экстремистских преступлений используются и такие мессенджеры, как Viber, WhatsApp и Telegram. Это связано в первую очередь с тем, что обозначенные программы обладают функцией шифрования, что защищает файлы от отслеживания и взлома без использования специальных программ.

Информационно-коммуникационные сети стали основным средством общения для экстремистских и террористических организаций: они используются ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений, распространения экстремистской идеологии. Основной проблемой для следственных органов является длительность процесса получения информации с защищенных сайтов и их блокировки.

Способ совершения преступлений обусловлен большими возможностями информационных технологий. Местом совершения преступления экстремистского характера может стать любая точка, где есть доступ к сети Интернет.

Действия следователя на первоначальном и последующем этапах во многом зависят от характера совершенного преступления, но, как правило, перечень обязательных для выполнения мероприятий всегда остается неизменным. Так, при обнаружении информации, формально содержащей признаки экстремизма, следователю либо иному

лицу необходимо ее процессуально зафиксировать, ведь в последующем это может послужить основанием для возбуждения уголовного дела. Как правило, в практической деятельности следователь в роли лица, обнаружившего указанное преступление, выступает крайне редко. Чаще всего ему поступает либо материал проверки для последующего принятия процессуального решения, либо уже возбужденное уголовное дело. В обоих случаях необходимо процессуально зафиксировать сам факт совершенного преступления, если этого не сделано ранее. Важным является в кратчайшие сроки провести осмотр, отразив данный факт в протоколе осмотра места происшествия. При производстве указанного следственного действия и использовании в качестве объекта какого-либо интернет-ресурса следователю необходимо указывать все возможные реквизиты последнего: электронный адрес, наименование, сведения об обратной связи, контакты и т. д. В обязательном порядке к протоколу следственного действия прилагаются изображения ресурса, фиксируется содержание размещенных сведений.

Особое внимание следователю необходимо уделять взаимодействию с оперативными подразделениями органов внутренних

дел, так как некоторые аспекты совершенного преступления невозможно установить без их помощи.

Второй блок алгоритма расследования преступления образуют следственные действия, проводимые с лицами, а также материальными носителями информации. Они выходят на первый план при установлении лица, совершившего преступление, свидетелей и заключаются в сборе объема доказательственной информации. К таким следственным действиям можно отнести допросы свидетелей, обыски и выемки на местах совершения преступлений, назначение различных экспертиз, в основном компьютерных и лингвистических, проведение очных ставок, осмотров, допросов. На данном этапе расследование упрощается тем, что, как правило, в уголовном деле уже содержатся материалы о лице, совершившем преступление, характере последствий, и следователю остается только в общепределенном порядке собрать максимально возможную доказательственную базу.

Быстрое развитие информационно-коммуникационных систем, появление программ, способных шифровать информацию, осложняют процесс выявления и доказывания преступлений экстремистского характера.

## СПИСОК ЛИТЕРАТУРЫ

1. Бутенко, А. С. Экстремизм в сети Интернет: понятие и сущность / А. С. Бутенко // Юристъ-Правоведъ. – 2019. – № 2. – С. 57–61.
2. Валеев, А. Х. Борьба с проявлением экстремизма в сети Интернет / А. Х. Валеев // Бизнес в законе. – 2011. – № 6. – С. 125–127.
4. Зубкина, О. С. Экстремизм в современном интернет-пространстве / О. С. Зубкина // Ростовский научный журнал. – 2019. – № 1. – С. 48–54.
5. Тронева, В. Н. Проблема распространения экстремизма в интернет-среде / В. Н. Тронева // Научный вестник Волгоградского филиала РАНХиГС. Серия : Юриспруденция. – 2019. – № 2. – С. 85–89. – URL: <https://www.elibrary.ru/item.asp?id=42326823> (дата обращения: 08.08.2020).
6. Тхакохов, А. А. К проблеме молодежного экстремизма: факторы распространения, особенности, способы борьбы / А. А. Тхакохов // Молодой ученый. – 2015. – № 4. – С. 481–482.

## REFERENCES

1. Butenko A. S. Ekstremizm v seti Internet: ponyatie i sushchnost' [Extremism on the Internet: concept and essence]. *YUrist»-Pravoved» – Lawyer-Legist*, 2019, no. 2, pp. 57–61. (In Russ.).
2. Valeev A. H. Bor'ba s proyavleniem ekstremizma v seti Internet [Fight against manifestations of extremism on the Internet]. *Biznes v zakone – Business in law*, 2011, no. 6, pp. 125–127. (In Russ.).
4. Zubkina O. S. Ekstremizm v sovremennom internet-prostranstve [Extremism in the modern Internet space]. *Rostovskiy nauchnyy zhurnal – Rostov scientific journal*, 2019, no. 1, pp. 48–54. (In Russ.).
5. Troneva V. N. Problema rasprostraneniya ekstremizma v internet-srede [The problem of the spread of extremism in the Internet environment]. *Nauchnyy vestnik Volgogradskogo filiala RANHiGS. YUrisprudenciya – Scientific bulletin of the Volgograd branch of the RANHiGS. Jurisprudence*, 2019, no. 2, pp. 85–89. Available at: <https://www.elibrary.ru/item.asp?id=42326823> (accessed 08.08.2020). (In Russ.).
6. Thakohov A. A. K probleme molodezhnogo ekstremizma: faktory rasprostraneniya, osobennosti, sposoby bor'by [On the problem of youth extremism: factors of spread, features, methods of struggle]. *Molodoj uchenyj – Young scientist*, 2015, no. 4, pp. 481–482. (In Russ.).

## ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTORS

**НИНА ИГОРЕВНА ГЕРАСИМЕНКО** – старший преподаватель кафедры криминалистики Омской академии МВД России, г. Омск, Российская Федерация, кандидат юридических наук. ORCID: <https://orcid.org/0000-0002-1107-5337>, e-mail: [ninella007@mail.ru](mailto:ninella007@mail.ru)

**NINA I. GERASIMENKO** – Senior Lecturer of the Department of Criminalistics of the Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk, Russian Federation, PhD. in Law. ORCID: <https://orcid.org/0000-0002-1107-5337>, e-mail: [ninella007@mail.ru](mailto:ninella007@mail.ru)