

Научная статья
УДК: 343.985.7

ДЕСТРУКТИВНЫЕ ГРУППЫ В ГИБРИДНОЙ РЕАЛЬНОСТИ: МЕТОДОЛОГИЯ КЛАССИФИКАЦИИ И ОПЕРАТИВНО-РОЗЫСКНОЙ ИДЕНТИФИКАЦИИ

Сергей Владимирович Тимофеев¹, Александр Сергеевич Самоделкин²

¹Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, tsv.1981@mail.ru

²Московский университет МВД России им. В. Я. Кикотя, г. Москва, Российская Федерация, putin@list.ru

Аннотация. В статье исследуется феномен деструктивных групп в теоретическом и практическом плане. Осуществлены классификация и построение оперативно-розыскной характеристики деструктивных групп, функционирующих преимущественно в сети Интернет. На основе системного анализа проводится критический обзор существующих типологий и выявляются их ограничения. Авторы предлагают многоуровневую классификационную модель, интегрирующую целевой, функционально-ролевой, коммуникационно-поведенческий и технологический критерии. В рамках методологии разрабатывается структура оперативно-розыскной характеристики деструктивной интернет-группы как информационной модели, включающая параметры целеполагания, контента, социальной динамики, технологической инфраструктуры и криминалистически значимых признаков.

Ключевые слова: деструктивные группы, сеть Интернет, цифровая среда, оперативно-розыскная характеристика, методология, интернет-платформы, криминалистическая характеристика, информационно-аналитическая модель, сетевые сообщества.

Для цитирования: Тимофеев, С. В., Самоделкин, А. С. Деструктивные группы в условиях гибридной реальности: методологические основания классификации и идентификации // Криминалистика: вчера, сегодня, завтра. 2026. Т. 39. № 3. С. 145–159.

DESTRUCTIVE GROUPS IN HYBRID REALITY: METHODOLOGICAL FOUNDATIONS OF CLASSIFICATION AND IDENTIFICATION

Sergey V. Timofeev¹, Alexander S. Samodelkin²

¹East Siberian Institute of the MIA of Russia, Irkutsk, Russian Federation, tsv.1981@mail.ru

²Kikot Moscow University of the MIA of Russia, Moscow, Russian Federation, putin@list.ru

Abstract. The article examines the phenomenon of destructive groups in theoretical and practical terms. A classification and an operational-search characteristic of destructive groups functioning primarily on the Internet are developed. Based on a systematic analysis, a critical review of existing typologies

is carried out and their limitations are identified. The authors propose a multi-level classification model integrating target, functional-role, communicative-behavioral, and technological criteria. Within the framework of the methodology, the structure of the operational-search characteristic of a destructive Internet group is developed as an information model, including parameters of goal-setting, content, social dynamics, technological infrastructure, and forensically significant features.

Keywords: destructive groups, Internet, digital environment, operational-search characteristic, methodology, Internet platforms, forensic characteristics, information-analytical model, network communities

For citation: Timofeev S.V., Samodelkin A.S. Destruktivnyye gruppy v usloviyakh gibridnoy real'nosti: metodologicheskiye osnovaniya klassifikatsii i identifikatsii [Destructive groups in the conditions of hybrid reality: methodological foundations of classification and identification]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2026, vol. 39. no. 3, pp. 145–159 (in Russ.).

Введение

Феномен деструктивных групп в сети Интернет представляет собой одну из наиболее опасных угроз современному обществу. Глобальная сеть, изначально создававшаяся как инструмент свободного обмена информацией, превратилась в благодатную среду для распространения идеологий ненависти, насилия и саморазрушения. Виртуальные сообщества, используя методы психологического манипулирования, способны подтолкнуть несовершеннолетних к совершению поступков, приводящих к необратимым последствиям – от агрессии в отношении окружающих до добровольного ухода из жизни.

Отдельного внимания заслуживает способность подобных групп к быстрой трансформации, смене вывесок и подстройке под изменяющиеся условия. Их организаторы целенаправленно эксплуатируют психологическую уязвимость молодежной аудитории, подменяют традиционные нравственные ориентиры псевдоценностями, создают иллюзию избранности. Именно это делает деструктивные сообщества привлекательными для подростков, находящихся в поиске собственной иден-

тичности и общественного признания. Разрушительное воздействие таких групп не ограничивается рамками виртуального пространства – оно неизбежно проецируется на реальные социальные связи, дестабилизирует семейные отношения, калечит судьбы и создает прямые угрозы общественной безопасности.

Масштаб явления диктует необходимость пересмотра существующих подходов к его осмыслению. Традиционные классификационные схемы, разработанные для анализа офлайн-сообществ, оказываются малопригодными в условиях цифровой реальности, где границы между виртуальным и реальным стремительно стираются.

Статистика подтверждает тревожную динамику. По сведениям Роскомнадзора, в 2024 году доступ к интернет-ресурсам был ограничен в отношении 810,5 тыс. материалов, признанных противоправными. В 2025 году количество таких ограничений выросло на 59 % и составило уже 1,289 млн единиц контента. Мониторинг охватывал основные российские и зарубежные цифровые площадки и социальные сети «ВКонтакте», «Одноклассники», «Мой мир»,

платформу «Ответы Mail.ru», видеохостинги Rutube и TikTok, сервис Likee, а также мессенджер Telegram.

Наиболее значительный рост блокировок в 2025 году зафиксирован в отношении материалов, связанных со средствами обхода блокировок – их количество увеличилось на 1235 % и превысило 93 тыс. Существенно возросло и число ограничений доступа к контенту, признанному экстремистским – на 269 % (до 170,3 тыс. материалов). Кроме того, на 190 % (до 18,7 тыс.) выросло число блокировок материалов с детской порнографией; на 80 % (до 229,3 тыс.) – с пронаркотическим контентом; на 60 % (до 52,2 тыс.) – с вовлечением несовершеннолетних в противоправную деятельность.

В Роскомнадзоре для мониторинга и анализа контента задействованы три автоматизированные системы. «Мир» осуществляет сбор и анализ текстовой информации, «Окулус» предназначен для выявления и идентификации изображений и видеоматериалов, а «Вебрь» дополняет их прогнозной аналитикой¹.

К. Ясперс отмечал: «любая классификация, представляющая собой не просто слабо структурированную группировку данных, а нечто большее, содержит в себе объективное суждение; сама по себе она уже предполагает выбор определенной мировоззренческой установки» [1, с. 15]. Это суждение, высказанное в контексте психопатологии, приобретает особую эвристическую ценность применительно к деструктивным группам в интернете.

При этом современные исследователи и практики сталкиваются с феноменом, который сложно сгруп-

пировать и классифицировать. Это связано с тем, что виртуальные сообщества обладают высокой лабильностью, маскируются под легитимные объединения, используют алгоритмические ленты социальных сетей для камуфляжа своих целей. Они способны в течение нескольких дней менять название, платформу и систему кодов и символов.

Верным представляется мнение М. Кастельса, что сетевое общество представляет собой «социальную структуру, построенную на сетях, активируемых микроэлектронными технологиями, основанными на цифровой информации и коммуникационных технологиях» [2, с. 45]. Деструктивные онлайн-сообщества стали органичной, хотя и патологической, частью этой структуры. Их изучение требует выработки принципиально нового методологического подхода.

Исследователи все чаще обращают внимание на то, что деструктивные интернет-группы являются закономерным продуктом трансформации коммуникационных практик в условиях цифровой реальности.

Е. В. Сусименко и А. В. Хорохордина обоснованно указывают, что «медиатизация становится фундаментальным процессом, трансформирующим практически все аспекты социальной жизни, при этом ее деструктивные эффекты проявляются на когнитивном, психологическом, социокультурном и институциональном уровнях» [3, с. 108].

В этих условиях оперативно-розыскная практика зачастую отстает в осмыслении данного феномена. Она оперирует разрозненными эмпирическими наблюдениями без единой методологической базы, адаптированной именно к интернет-реалиям.

Поэтому особую актуальность приобретает разработка универсальной методологии классификации и

¹ «Ведомости»: РКН увеличил количество удаленных запрещенных материалов на 59% [Электронный ресурс] URL : <https://tass.ru/obschestvo/26181237> (дата обращения 25.05.2026).

идентификации деструктивных интернет-групп.

Как справедливо замечает К. А. Шуликов, «информация способна оказывать организующее, управленческое воздействие на ее потребителей» [4, с. 177].

В. И. Красиков и Е. В. Фоменко в своем исследовании предприняли попытку «выявления и типологизации наиболее резонансных «групп ненависти», существующих в настоящее время в Рунете». В итоге ими был разработан «категориально-критериальный аппарат для выявления радикальных неполитических интернет-сообществ», установлены адресования их интернет-распространения, сопоставлены их общие и отличные признаки, определена шкала их социальной вредности. Авторы отмечают, что в последние два десятилетия «появились новые радикальные интернет-сообщества, которые мотивированы в своем появлении другими важными аспектами человеческого существования, помимо политического, националистического или религиозного. Такими, как гендерный, возрастной, личностно-психологический и др.». Их роднит с политическими формами радикализма «интенсивно проявляющиеся в их активности профили ненависти к определенным группам людей» [5, с. 6]. Отличает же их отсутствие определяющей политической вовлеченности.

Использование этих данных требует не только правового, но и методологического обеспечения, позволяющего превращать хаотичный поток цифровых данных в структурированную оперативную картину.

Президент Российской Федерации В. В. Путин неоднократно подчеркивал необходимость наращивать усилия по пресечению распространения деструктивного контента в интернете, что повлекло изменения в

действующем уголовном законодательстве Российской Федерации².

Все вышеизложенное обуславливает необходимость разработки целостного методологического подхода к классификации и построению оперативно-розыскной характеристики деструктивных групп, действующих в сети Интернет. Такой подход должен интегрировать достижения криминалистики, оперативно-розыскной деятельности, интернет-лингвистики и социальной психологии сетевых групп.

Цель настоящего исследования заключается в разработке целостного методологического подхода к классификации и построению оперативно-розыскной характеристики деструктивных групп, действующих в сети Интернет, а также обоснование практической значимости предлагаемой модели для оптимизации деятельности оперативных подразделений органов внутренних дел в киберпространстве.

Основная часть

Прежде чем перейти к непосредственному анализу деструктивных интернет-сообществ, необходимо дать научное определение ключевого понятию исследования.

В научной литературе сложилось понимание вредной информации как сведений, «негативное воздействие которых на индивидуальную психику и общественное сознание обуславливает необходимость ограничения или запрета их оборота в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности

² В УК РФ внесены изменения, направленные на противодействие распространению деструктивного контента / Президент России. URL : <http://www.kremlin.ru/catalog/keywords/6/events/74774> (дата обращения 25.05.2026).

государства»³. Применительно к интернет-среде указанное понятие конкретизируется через категорию «контент» – информационно-значимое наполнение сети Интернет, включающее тексты, графику, мультимедиа и иные формы представления данных⁴.

Деструктивная группа в сети Интернет в настоящем исследовании понимается как устойчивое или ситуативно возникающее онлайн-сообщество, чья деятельность полностью или преимущественно разворачивается на интернет-платформах, в социальных сетях, мессенджерах, на форумах или в иных сегментах глобальной сети в целях причинения вреда личности, обществу или государству путем распространения противоправного контента, психологического манипулирования, координации противоправных действий либо создания условий для их совершения.

Ключевой признак такой группы – использование интернет-пространства в качестве основной арены функционирования. Это отличает ее от традиционных преступных сообществ, для которых сеть является лишь вспомогательным средством коммуникации.

³ Информация по делу № 02а-1886/2025 /Информация по административным делам первой инстанции // Информация по судебным делам /// Процесс //// Симоновский районный суд. Официальный портал судов общей юрисдикции города Москвы [Электронный ресурс] URL : <https://www.mos-gorsud.ru/rs/simonovskij/services/cases/kas/details/536dffc0-5b04-11f0-aa34-b1b3a628812a?caseNumber=2a-1886/25> (дата обращения 25.05.2026).

⁴ Верховный Суд Российской Федерации признал «Колумбайн» террористической организацией / Генеральная прокуратура Российской Федерации [Электронный ресурс] URL : <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/main/e480267/?ysclid=mr7hefyijq405902439> (дата обращения 25.05.2026).

Анализ научной литературы и правоприменительной практики позволил выделить сущностные характеристики деструктивных интернет-групп.

В основе существования группы лежит противоправная направленность в виде идеологии, противоречащей ценностям общества и государства, деформирующая нравственный облик личности и проявляющаяся в противоправном поведении.

Цель таких групп – манипулирование сознанием людей, подталкивание к опасным действиям, навязывание определенных взглядов.

Нам импонирует точка зрения И. В. Носова, который утверждает, что «в социальной сфере социальные сети привели к переосмыслению сути и динамики дружбы, поскольку незнакомцы и знакомые теперь могут быть добавлены в качестве «друзей», что ведет к разрушению основных социальных норм и физической дистанции, которые ранее определяли человеческие взаимодействия» [6, с. 58].

Помимо идеологической направленности, деструктивные интернет-группы характеризуются организованностью, наличием определенной структуры (иерархической, сетевой или ризоматической), распределением ролей и функций между участниками, системой внутренней коммуникации и координации.

Деятельность таких групп имеет деструктивный характер и направлена на причинение морального, психологического, физического или материального вреда отдельным лицам, социальным группам или обществу в целом.

Существенной особенностью является использование интернет-среды как основной платформы. При этом деятельность группы полностью или преимущественно осуществляется в цифровом пространстве, что определяет специфику ее

организации, коммуникации и способов воздействия.

Важнейшими характеристиками выступают высокая динамичность и адаптивность, способность быстро изменять структуру, тактику, платформы и контент в ответ на внешние воздействия, а также анонимность и псевдонимность участников, достигаемые использованием никнеймов, сервисов анонимизации, прокси-серверов и зашифрованных мессенджеров.

Кроме того, деструктивные интернет-группы отличаются мультиплатформенностью, т. е. использованием нескольких интернет-площадок для разных целей:

- координации в мессенджерах;
- пропаганды в социальных сетях;
- хранения файлов на облачных сервисах;
- финансирования через криптовалюты.

Деструктивный контент обладает свойством виральности распространения (способностью материала стремительно набирать популярность, словно вирус, захватывая внимание всё большего числа людей за короткое время). Он может мгновенно распространяться через алгоритмы рекомендаций и репосты, многократно усиливая охват аудитории без активных действий самих участников.

Наконец, трансграничность, когда участники могут находиться в различных юрисдикциях, что затрудняет правовую квалификацию и оперативное реагирование.

На основе выделенных характеристик предлагается следующее определение деструктивной группы в сети Интернет – это организованное онлайн-сообщество, объединенное идеологией, противоречащей конституционным ценностям и нормам морали, деятельность которого направлена на причинение вреда личности, обществу или государству

посредством распространения противоправного контента, психологического манипулирования, координации противоправных действий либо создания условий для их совершения, с использованием интернет-платформ, социальных сетей, мессенджеров и иных сегментов глобальной сети в качестве основной среды функционирования, характеризующееся высокой динамичностью, анонимностью участников, мультиплатформенностью и трансграничностью.

Сегодня исследователь и практик сталкиваются с феноменом, который сопротивляется простой «группировке данных». Виртуальные сообщества экстремистской, террористической, суицидальной или иной деструктивной направленности обладают высокой лабильностью, маскируются под легитимные объединения и используют алгоритмические ленты социальных сетей для камуфляжа своих целей.

Указанные особенности требуют пересмотра традиционных подходов к классификации и описанию таких групп, поскольку статические модели, разработанные для офлайн-сообществ, оказываются малоприменимыми в динамичной интернет-среде.

В научной литературе представлен ряд попыток классифицировать деструктивные сообщества в сети. Наиболее распространены следующие подходы:

1) основанные на целевом (идеологическом) признаке, представленные как выделение экстремистских, террористических, суицидальных, сектантских, киберпреступных групп и т. д.;

2) на платформенном признаке – это классификация по типу используемой интернет-платформы (социальные сети, мессенджеры, форумы, Darknet);

3) по степени публичности или закрытости – от полностью откры-

тых публичных сообществ до глубоко законспирированных ячеек в зашифрованных каналах.

Каждый из этих подходов имеет ценность, но и существенные ограничения применительно к интернет-среде.

Классификация по цели, будучи содержательно ясной, часто оказывается слишком общей и не отражает оперативно значимых особенностей структуры и коммуникаций в сети.

Платформенный подход полезен для выбора тактики мониторинга, но не отвечает на вопрос о сущности группы и ее деструктивном потенциале.

Деление по степени закрытости является важным, но вторичным тактическим параметром, поскольку в интернете группы могут оперативно менять режим доступа.

Особого внимания заслуживает концепция «групп ненависти», исследованных В. И. Красиковым и Е.В. Фоменко, предлагающих категориально-критериальный аппарат для выявления радикальных неполитических интернет-сообществ – маскулистов, радфем, скулшутеров, троллей, догхантеров и иных объединений, мотивированных не политическими, а гендерными, возрастными и личностно-психологическими факторами [7, с. 6–7].

Данный подход особенно релевантен для интернет-среды, где такие группы активно используют анонимность и алгоритмическое продвижение для привлечения аудитории, и может быть интегрирован в предлагаемую ниже классификационную модель.

Практика противодействия деструктивным интернет-сообществам демонстрирует многообразие их проявлений. Так, в 2025 году Симоновский районный суд Москвы признал вредными для подростков семь крупных сообществ во «ВКонтакте» с аудиторией, превышающей 700 ты-

сяч подписчиков, таких как: «Borzz», «BLATATA», «Бандитский двор», «Культурное движение», «ZDRAVIYDVIZH», «Бог спасет, братва поможет» и «Бог простит, а я запомню». Суд установил, что публикации в этих группах пропагандировали асоциальное поведение, склоняли подростков к употреблению алкоголя, наркотиков, курению, азартным играм, проституции, бродяжничеству и попрошайничеству⁵. Данный пример иллюстрирует, как деструктивные группы могут маскироваться под «околокриминальные» паблики, используют привлекательную для молодежи стилистику и формируя искаженное представление о социальных нормах.

Особую опасность, как подчеркивает в своем исследовании Е. М. Тимошина, «представляет вовлечение молодежи через сеть Интернет в группы деструктивной направленности, где очень активно используются социальные сети». Ученый описывает стратегию «постепенного погружения» детей в деструктивный контент как способ их вовлечения в деструктивные субкультуры. По ее мнению, особенность вовлечения детей в такие субкультуры заключается в стратегии «постепенного погружения» в деструктивный контент. Эксперты называют это «воронкой вовлечения». Наиболее наглядна для понимания аналогия с матрешкой, «в которой самая большая – это видимая

⁵ Информация по делу № 02а-1886/2025 / Информация по административным делам первой инстанции // Информация по судебным делам /// Процесс //// Симоновский районный суд ///// Официальный портал судов общей юрисдикции города Москвы [Электронный ресурс] URL : <https://www.mosgorsud.ru/rs/simonovskij/services/cases/kas/details/536dffc0-5b04-11f0-aa34-b1b3a628812a?caseNumber=2a-1886/25> (дата обращения 25.05.2026).

всем фигура, наиболее безобидная, а каждая последующая меньшая матрешка – уровень более опасный». «Максимально опасный уровень – самая маленькая матрешка – представляет своего рода «дно аморальных ценностей»» [8, с. 287–289]. Каждый последующий уровень – более закрытый, попасть в него можно лишь по специальному приглашению – ссылке.

Не менее показательным является уголовное дело о «группе смерти», раскрытое Следственным комитетом России в 2025 году, жертвами которой стали 20 детей из разных регионов страны. Организаторами оказались житель Новосибирска и несовершеннолетняя девушка из Ярославля, которые целенаправленно искали в социальных сетях подростков, интересующихся мрачной тематикой, и вовлекали их в опасную игру по схеме, напоминающей печально известный «Синий кит»⁶. Фигуранты давали детям психологически разрушительные задания, постепенно подводя их к мыслям о суициде, причем не извлекали никакой материальной выгоды – их мотивом было самоутверждение. Суд приговорил мужчину к 10 годам колонии. Этот случай подтверждает тезис о том, что деструктивные интернет-группы могут не иметь корыстной мотивации, что существенно отличает их от традиционных преступных сообществ и требует особых подходов к выявлению и оперативно-розыскному документированию.

Верховный Суд Российской Федерации в 2022 году признал движение «Колумбайн» (скулшутинг) тер-

рористическим и запретил его на территории России. В социальных сетях создаются тематические группы скулшутинга, осуществляется психологическая обработка по снятию у молодежи и подростков морального запрета на применение насилия и совершение убийств. За организацию либо участие в деятельности террористической организации предусмотрена уголовная ответственность вплоть до пожизненного лишения свободы⁷.

Для преодоления выявленных ограничений предлагается четырехуровневая классификационная модель, интегрирующая взаимосвязанные критерии применительно к интернет-сообществам. Эта модель позволяет перейти от простой *таксономии* к построению оперативно значимого *профиля группы в сети Интернет*.

Первый уровень – целевой (содержательно-идеологический). Он определяет смысловое ядро группы и мотивацию участников в интернете.

В рамках данного уровня выделяются политико-идеологические интернет-группы, включающие экстремистские, сепаратистские и террористические объединения, использующие сеть для пропаганды, вербовки, координации и финансирования; социально-деструктивные интернет-группы, пропагандирующие насилие (скулшутинг, буллинг), суицид (про-ау-сообщества), расстройства пищевого поведения; криминально-экономические интернет-группы, организованные для кибермошенничества, торговли запрещенными товарами, отмывания денег через криптовалюты, а также деграда-

⁶ МК.РУ: В Москве раскрыли дело "группы смерти", в которую заманивали детей - Российская газета [Электронный ресурс] URL : <https://rg.ru/2025/07/26/mkru-v-moskve-raskryli-delo-gruppy-smerti-v-kotoruiu-vovlekalis-deti.html> (дата обращения 25.05.2026).

⁷ Верховный Суд Российской Федерации признал «Колумбайн» террористической организацией [Электронный ресурс] URL : <https://epp.genproc.gov.ru/ru/gprf/mass-media/news/archive/e480267/> (дата обращения 25.05.2026).

ционно-маргинальные интернет-группы, культивирующие асоциальный образ жизни и ненависть к отдельным социальным категориям.

Второй уровень – функционально-ролевой и структурный. Этот уровень описывает внутреннюю организацию интернет-группы и распределение функций в цифровой среде. Здесь выделяются централизованные (иерархические) структуры с четким лидером и вертикалью подчинения, характерные для традиционных экстремистских организаций, перенесших свою деятельность в сеть; децентрализованные (сетевые) структуры, состоящие из относительно автономных ячеек или отдельных активистов, связанных общей идеологией через интернет-платформы, но не имеющих единого командного центра; а также ризоматические (климатические) структуры, не имеющие постоянной организации и формирующиеся стихийно вокруг конкретного события или информационного повода в социальных сетях.

Третий уровень – коммуникационно-поведенческий. На этом уровне анализируются паттерны взаимодействия внутри интернет-группы и с внешней средой, оцениваются степень конспирации в сети – от открытых публичных групп до полностью закрытых частных каналов; характер коммуникации – агрессивно-вербовочный, направленный на вовлечение новых участников, дискуссионно-идеологический, поддерживающий внутреннюю идентичность, либо инструментально-координационный, связанный с обсуждением планов действий; а также используемые культурные коды – специфический интернет-сленг, мемы, символика, эмодзи, ритуалы, формирующие групповую идентичность в сети и служащие маркерами «свой – чужой».

Четвертый уровень – технологический-инфраструктурный. На этом уровне

анализируются цифровые инструменты и интернет-площадки, задействованные в деятельности группы. В расчет берется тип платформы: социальные сети, мессенджеры, тематические форумы, игровые чаты или ресурсы в Darknet. Важным элементом выступает и стратегия присутствия в сети: наличие основного узла (центрального ресурса) и вспомогательных каналов, распределяющих разные функции.

Существенное уточнение вносит разграничение контент-рисков (связанных с ознакомлением пользователей с уже размещенной деструктивной информацией в интернете) и коммуникационных рисков (возникающих в процессе межличностного взаимодействия в сети и связанных с использованием манипулятивных речевых стратегий), предложенное Е. И. Галяшиной и В. Д. Никишиным [9, с. 85–86].

Это различие позволяет дополнить классификацию интернет-групп критерием преобладающего типа деструктивного воздействия, что особенно важно для групп вербовочной направленности, активно использующих личные сообщения и чаты.

Данная многоуровневая модель позволяет не просто отнести интернет-группу к категории, а построить ее комплексный сетевой профиль, например: «политико-идеологическая (экстремистская) интернет-группа децентрализованной сетевой структуры с высокой степенью конспирации и агрессивно-вербовочным типом коммуникации, базирующаяся на платформе Telegram с использованием базового шифрования».

Разработанная классификация служит основой для построения оперативно-розыскной характеристики интернет-группы для систематизированного описания сообщества в параметрах, имеющих значение при решении задач оперативно-

розыскной деятельности, связанных с выявлением, документированием прогнозирования и пресечения преступной деятельности деструктивных групп.

Оперативно-розыскная характеристика (далее – ОРХ) в предлагаемой трактовке *представляет собой динамическую информационную модель, систематизирующую сведения о деструктивном онлайн-сообществе в параметрах, имеющих оперативно-тактическое, доказательственное и прогностическое значение в цифровой среде.*

В отличие от криминалистической характеристики, которая ориентирована преимущественно на ретроспективное установление механизма преступления и идентификацию слеодообразующих объектов в материальном мире, ОРХ интернет-группы имеет выраженную прогностическую и управленческую направленность и важна для обоснования оптимального выбора гласных и негласных методов и средств, определения наиболее эффективных в этих случаях оперативно-розыскных мероприятий в сети Интернет, а также для оценки динамики угрозы и планирования тактических оперативных комбинаций в киберпространстве.

Предлагаемая структура ОРХ для интернет-группы включает шесть взаимосвязанных элементов, адаптированных к специфике глобальной сети.

Первый элемент. Установочные и идентификационные данные в интернете, содержащие наименование (самоназвание) группы, используемые хэштеги, слоганы, никнеймы участников; цифровые адреса – URL, как основного ресурса, ссылки на спутниковые каналы, аккаунты администраторов и ключевых фигур; а также время возникновения в сети и ключевые этапы развития.

Второй элемент. Целеполагание и идеологическое содержание вклю-

чают формализованную цель и идеологию группы, транслируемые через интернет-контент; целевую интернет-аудиторию для вербовки с ее социально-демографическим и психологическим портретом; а также основные нарративы, образы врага и символический аппарат, используемые в сетевых публикациях.

Третий элемент. Социально-сетевая структура и ролевое распределение, описывающие тип структуры в интернете, карту социальных связей (SNA-граф) с выделением ключевых фигур в сети – лидеров, идеологов, технических администраторов, активных распространителей, рядовых участников – и функции каждой роли в группе, проявляющиеся через характер цифровых следов.

Четвертый элемент. Коммуникативные и поведенческие паттерны в интернете. Он анализирует характер контента (тексты, мемы, видео, аудио, ссылки на внешние ресурсы); частоту и время активности, реакцию на внешние события в реальной жизни и в цифровой среде (информационные триггеры); используемые методы вербовки и манипуляции в сети – техники ментального принуждения, «ловушки вовлечения», приемы социальной инженерии; а также признаки планирования конкретных противоправных действий через интернет – использование кодовых слов, зашифрованных сообщений, обсуждение места и времени в частных чатах.

Пятый элемент. Технико-технологическая инфраструктура в интернете. Он содержит информацию об используемом софте и аппаратных средствах, задействованных в коммуникации; сведения о способах обеспечения анонимности и безопасности в сети (шифрование, прокси-серверы, анонимные браузеры, и т. п.); а также каналы финансирования через интернет – краудфандинг, криптовалюты, анонимные платежные системы.

Наконец, *шестой элемент* – это криминалистически значимые признаки и угрозы в цифровой среде, включающие конкретные составы преступлений, признаки которых содержатся в деятельности интернет-группы.

Например, ст. 280, 280.1, 282, 205.2 УК РФ и другие. Также этот элемент содержит оценку уровня общественной опасности и потенциала насилия на основе анализа сетевого контента и коммуникаций; а также прогноз развития ситуации – скейлинг активности в сети, риски перехода к реальным действиям, возможное распространение на другие интернет-платформы.

Как справедливо отмечает В. С. Овчинский, «оперативно-розыскная характеристика из описательного документа должна превратиться в аналитический инструмент, позволяющий не только констатировать, но и моделировать поведение группы» [10, с. 15]. Именно такой подход реализует предложенная структура применительно к интернет-группам, обеспечивая переход от пассивного описания к активному прогнозированию и тактическому планированию в цифровой среде.

При этом ОРХ интернет-группы может быть дополнена элементом лингвистических и семиотических особенностей деструктивного дискурса в сети – использованием специфических культурных кодов, интернет-сленга, символики, эмодзи-кодов, а также частотных словарей негативно окрашенных понятий, что позволяет автоматизировать мониторинг социальных сетей и повысить эффективность идентификации групп на ранних стадиях их формирования.

Особого внимания заслуживает вопрос о соотношении оперативно-розыскной и криминалистической характеристик применительно к интернет-группам.

Криминалистическая характеристика преступления традиционно по-

нимается как система типичных данных о способе, механизме, обстановке, субъекте и иных элементах преступного деяния, имеющих значение для его расследования. Применительно к интернет-среде криминалистическая характеристика фокусируется на цифровых следах, способах совершения преступлений в сети Интернет и признаках, позволяющих идентифицировать правонарушителя.

В отличие от нее, оперативно-розыскная характеристика деструктивной интернет-группы ориентирована не столько на уже совершенное деяние, сколько на выявление, документирование и прогнозирование противоправной активности сообщества в ее динамике на интернет-платформах.

Сходство между ними проявляется в том, что обе являются информационными моделями, систематизирующими криминалистически значимые признаки в цифровой среде; обе оперируют данными о субъектах, способах, орудиях и обстановке; обе служат основанием для выдвижения версий и планирования действий.

Вместе с тем данные различия носят принципиальный характер, и в условиях интернет-среды это проявляется наиболее отчетливо. Криминалистическая характеристика ориентирована на ретроспективу: она позволяет восстановить картину уже состоявшегося события через анализ оставленных в цифровом пространстве следов. Оперативно-розыскная характеристика, напротив, нацелена на работу с текущим состоянием сетевой группы, отслеживание ее изменений и построение прогнозов относительно дальнейших действий.

Криминалистическая характеристика строится на относительно устойчивых, повторяющихся моделях поведения и типовых признаках. ОРХ в силу высокой подвижности интернет-сообществ требует постоянного обновления – сетевое объединение способно за несколько часов сменить

площадку, наименование, состав активных участников и смысловые акценты в своей риторике.

По сути криминалистическая характеристика отвечает на вопросы: «что именно произошло?» и «кто мог быть причастен?». ОРХ же дает ответы на иного рода вопросы: «что в данный момент происходит в интернет-пространстве?», «в каком направлении эволюционирует группа?», «как на нее можно повлиять имеющимися оперативными средствами?».

Таким образом, оперативно-розыскная характеристика интернет-группы не подменяет собой криминалистическую характеристику, а органично дополняет и развивает ее с учетом специфики глобальной сети и задач оперативно-розыскной деятельности. Она превращает анализ в непрерывный процесс, позволяющий отслеживать изменения в режиме реального времени.

Вывод и заключение

В рамках проведенного исследования удалось сформировать единый методологический подход к анализу деструктивных интернет-сообществ. Его основу составляют два взаимосвязанных элемента: многоуровневая классификация и структурированная оперативно-розыскная характеристика.

Оба инструмента адаптированы к подвижной, быстро меняющейся цифровой среде и могут быть использованы как в теоретических разработках, так и в практической деятельности правоохранительных органов.

В результате системного анализа научной литературы и правоприменительной практики предложено научное определение деструктивной группы в сети Интернет.

В контексте исследования под ней понимается организованное онлайн-сообщество, объединенное идеологией, противоречащей конституционным ценностям и нормам

морали, деятельность которой направлена на причинение вреда личности, обществу или государству посредством распространения противоправного контента, психологического манипулирования, координации противоправных действий либо создания условий для их совершения, с использованием интернет-платформ, социальных сетей, мессенджеров и иных сегментов глобальной сети в качестве основной среды функционирования, характеризующееся высокой динамичностью, анонимностью участников, мультиплатформенностью и трансграничностью.

Классификация деструктивных интернет-групп, построенная по четырем взаимодополняющим критериям – целевому, функционально-ролевому, коммуникационно-поведенческому и технологическому – позволяет преодолеть ограничения одномерных типологий и строить комплексный сетевой профиль сообщества, отражающий его сущность, организацию, способы взаимодействия и технологическую базу в глобальной сети.

Оперативно-розыскная характеристика интернет-группы, структурированная в виде шести элементов, трансформируется из пассивного описания в активный аналитический инструмент, работающий в режиме реального времени. Ее сопоставление с криминалистической характеристикой показывает, что ОРХ имеет выраженный прогностический и управленческий характер, дополняя ретроспективную направленность криминалистической характеристики актуальной оценкой динамики интернет-сообщества и обоснованием тактических решений в киберпространстве.

Теоретическая значимость исследования заключается в систематизации знаний о деструктивных интернет-сообществах и интеграции методов из таких смежных областей,

как сетевой анализ, социальная психология сетевых групп, цифровая криминалистика, интернет-лингвистика в понятийный аппарат теории оперативно-розыскной деятельности.

Практическая ценность подхода состоит в том, что он предоставляет оперативным подразделениям четкий алгоритм анализа интернет-групп, позволяющий унифицировать и повысить качество информационно-аналитической работы в киберпространстве, ускорить оценку уровня угрозы, прогнозирование развития ситуации и обоснованный выбор ОРМ посредством мониторинга социальных сетей, легендирования, документирования цифровых следов, а также эффективно представлять результаты оперативной работы в виде результатов ОРД, которые после процессуальной проверки и оценки могут быть использованы в качестве доказательств, соответствующих требованиям УПК РФ.

Перспективным видится научно-практическая деятельность по разработке на основе предложенной методологии специализированного про-

граммного обеспечения или аналитических модулей для существующих систем мониторинга социальных сетей, автоматизирующих процесс заполнения и актуализации ОРХ интернет-групп в реальном времени.

Все это требует углубленного изучения вопросов эффективности различных тактик оперативно-розыскного противодействия применительно к группам разных классификационных типов в интернете, а также разработки единого междисциплинарного подхода, объединяющего достижения криминалистики, оперативно-розыскной деятельности, интернет-лингвистики и социальной психологии сетевых сообществ.

Для борьбы с деструктивными группами в сети Интернет предложенная методология может быть эффективным инструментом для сбора, систематизации и анализа такого знания, превращая хаотичный поток цифровых данных в четкую оперативную картину, необходимую для обеспечения решения задач ОРД, обеспечения законности и безопасности в цифровую эпоху.

СПИСОК ИСТОЧНИКОВ

1. *Jaspers, K.* Allgemeine Psychopathologie. Berlin: Springer, 1913. 420 s.
2. *Castells, M.* The Rise of the Network Society. The Information Age: Economy, Society, and Culture. Vol. I. Oxford: Blackwell, 2010. 594 p.
3. *Сусименко, Е. В., Хорохордина, А. В.* Деструктивные эффекты медиатизации сфер общественной жизни: формы, виды и классификации // Гуманитарий Юга России. 2025. Т. 14. № 3. С. 107–120.
4. *Шуликов, К. А.* Деструктивный контент: понятие, административно-правовая характеристика, виды // Вестник Санкт-Петербургского университета МВД России. 2023. № 2 (98). С. 176–183.
5. *Красиков, В. И., Фоменко, Е. В.* Группы ненависти в Рунете: ареалы интернет-распространения и типология // Вестник РПА. 2020. № 4. С. 5–27.
6. *Носова, И. В., Носов, Д. Д.* Деструктивный контент: цифровые угрозы и риски // Вестник СибГУТИ. 2025. Т. 19. № 2. С. 56–63.
7. *Красиков, В. И.* Группы ненависти в Рунете: ареалы интернет-распространения и типология / В. И. Красиков, Е. В. Фоменко // Вестник Российской правовой академии. 2020. № 4. С. 5–27.
8. *Тимошина, Е. М.* Деструктивные субкультуры несовершеннолетних как условия их виктимизации и криминализации // Ученые записки

Казанского юридического института МВД России. 2021. Т. 6, № 2 (12). С. 286–293.

9. Галяшина, Е. И., Никишин, В. Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // LEX RUSSICA. 2021. Т. 74. № 6 (175). С. 79–94.

10. Овчинский, В. С. Аналитика в киберпространстве: от данных к решениям // Информационное противодействие угрозам терроризма. 2023. № 15 (71). С. 10–19.

REFERENCES

1. Jaspers K. Allgemeine Psychopathologie. Berlin: Springer, 1913. 420 p.
2. Castells M. The Rise of the Network Society. The Information Age: Economy, Society, and Culture. Vol. I. Oxford: Blackwell, 2010. 594 p.
3. Susimenko E. V., Horohordina A. V. Destruktivnye efekty mediatizatsii sfer obshchestvennoy zhizni: formy, vidy i klassifikatsii [Destructive effects of the mediatization of spheres of public life: forms, types, and classifications]. Gumanitarij YUga Rossii. – Humanities of the South of Russia. 2025. Т. 14. №. 3. Pp. 107-120. (in Russian).
4. SHulikov K.A. Destruktivnyj kontent: ponyatie, administrativno-pravovaya harakteristika, vidy [Destructive content: concept, administrative-legal characteristics, and types]. Vestnik Sankt-Peterburgskogo universiteta MVD Rossii – Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2023. № 2 (98). Pp. 176-183. (in Russian).
5. Krasikov V.I., Fomenko E.V. Gruppy nenavisti v Runete: arealy internet-rasprostraneniya i tipologiya [Hate groups in Runet: areas of online spread and typology]. Vestnik RPA – Bulletin of the Russian Law Academy 2020. № 4. Pp. 5-27. (in Russian).
6. Nosova I.V., Nosov D.D. Destruktivnyj kontent: cifrovye ugrozy i riski [Destructive content: digital threats and risks]. Vestnik SibGUTI – Bulletin of SibGUTI. 2025. Т. 19. № 2. Pp. 56-63. (in Russian).
7. Krasikov, V. I., Fomenko E. V. Gruppy nenavisti v Runete: arealy internet-rasprostraneniya i tipologiya [Hate groups in Runet: areas of online spread and typology]. Vestnik Rossiyskoy pravovoy akademii – Bulletin of the Russian Law Academy. 2020. № 4. Pp. 5-27. (in Russian).
8. Timoshina E.M. Destruktivnye subkul'tury nesovershennoletnih kak usloviya ih viktimizatsii i kriminalizatsii [Destructive juvenile subcultures as conditions for their victimization and criminalization]. Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii – Scientific Notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2021. Т. 6. № 2 (12). Pp. 286-293. (in Russian).
9. Galyashina E.I., Nikishin V.D. Destruktivnoe rechevoe povedenie v cifrovoj srede: faktory, determiniruyushchie negativnoe vozdejstvie na mirovozzrenie pol'zovatelya [Destructive speech behavior in the digital environment: factors determining the negative impact on the user's worldview]. LEX RUSSICA. –LEX RUSSICA. 2021. Т. 74. № 6 (175). Pp. 79-94. (in Russian).

10. Ovchinskij V.S. Analitika v kiberprostranstve: ot dannyh k resheniyam [Analytics in cyberspace: from data to decisions]. Informacionnoe protivodejstvie ugrozam terrorizma. – Information Counteraction to Terrorism Threats 2023. № 15(71). Pp. 10-19. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Тимофеев Сергей Владимирович, кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности и специальной техники в органах внутренних дел. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, Иркутск, ул. Лермонтова, 110.

Самоделкин Александр Сергеевич, доктор юридических наук, доцент, профессор кафедры оперативно-разыскной деятельности и специальной техники. Московский университет МВД России имени В. Я. Кикотя. 117997, Российская Федерация, Москва, ул. Академика Волгина, д. 12.

INFORMATION ABOUT THE AUTHORS

Sergey V. Timofeev, Candidate of Law, Associate Professor, Associate Professor of the Department of Operational Investigative Activities and Special Equipment in Internal Affairs Bodies. East Siberian Institute of the MIA of Russia. 110 Lermontova St., Irkutsk, Russian Federation, 664074.

Alexander S. Samodelkin, Doctor of Law, Associate Professor, Professor of the Department of Operational-Investigative Activities and Specialized Equipment. Kikot Moscow University of the MIA of Russia. 12 Academician Volgina St., Moscow, Russian Federation, 117997.