СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА
ИМЕНИ А.Я. СУХАРЕВА

НАУЧНЫЕ ОСНОВЫ ГОСУДАРСТВЕННОЙ ПРОГРАММЫ БОРЬБЫ С КИБЕРЭКСТРЕМИЗМОМ

Всероссийский круглый стол,

посвященный памяти почетного профессора
Московской академии Следственного комитета
имени А.Я. Сухарева, почетного сотрудника Следственного
комитета Российской Федерации
Василия Васильевича Бычкова

4 апреля 2025 года

Москва, 2025

УДК 343
ББК 67.408

Н34 **Научные основы государственной программы борьбы с киберэкстремизмом:** материалы Всероссийского круглого стола, посвященного памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова (Москва, 4 апреля 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – 174 с.

Сборник сформирован по материалам, представленным участниками всероссийского круглого стола, проведенного в Московской академии Следственного комитета имени А.Я. Сухарева 4 апреля 2025 года. В круглом столе приняли участие представители разных вузов, практические работники из разных ведомств и ученые по научной специальности 5.1.4 – Уголовно-правовые науки.

Сборник предназначен для юристов – учёных и практиков, а также для всех тех, кто интересуется вопросами борьбы с экстремизмом и терроризмом, и в частности – с киберэкстремизмом.

Редакционная коллегия обращает внимание, что научные подходы, идеи и взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

Научные основы государственной программы борьбы с киберэкстремизмом

Всероссийский круглый стол, посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова

(Москва, 4 апреля 2025 г.)

В Московской академии Следственного комитета имени А.Я. Сухарева состоялся всероссийский круглый стол «Научные основы государственной программы борьбы с киберэкстремизмом», посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова.

В мероприятии приняли участие **Алексей Александрович Бессонов** – ректор Московской академии Следственного комитета имени А.Я. Сухарева, доктор юридических наук, доцент, генерал-майор юстиции; **Анатолий Михайлович Багмет –** заместитель руководителя Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации, кандидат юридических наук, доцент, генерал-майор юстиции; **Петр Андреевич Литвишко** – начальник управления правовой помощи и правоохранительного содействия Главного управления международно-правового сотрудничества Генеральной прокуратуры Российской Федерации, кандидат юридических наук, государственный советник юстиции 3 класса.

Модератор пленарного заседания – декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент подполковник юстиции **Армен Жораевич Саркисян**.

После открытия круглого стола А.А. Бессонов вручил памятный подарок почётному профессору Московской академии Следственного комитета Российской Федерации Владимиру Анатольевичу Прорвичу в честь его юбилея.

С докладами выступили: **Александр Фомич Волынский –** профессор кафедры судебно-экспертной и оперативно-разыскной деятельности факультета подготовки криминалистов Московской академии

Следственного комитета имени А.Я. Сухарева, профессор кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, профессор заслуженный деятель науки Российской Федерации, заслуженный юрист Российской Федерации, заслуженный работник МВД России.

Почетный профессор В.В. Бычков как пример служения России.

Прорвич Владимир Антонович – профессор-исследователь департамента уголовного права, процесса и криминалистики НИУ ВШЭ, доктор юридических наук, доктор технических наук, профессор, почётный профессор Московской академии Следственного комитета имени А.Я. Сухарева.

Использование принципа дополнительности при формировании юридических алгоритмов доказывания по уголовным делам о киберпреступлениях в сфере экстремизма.

Харченко Сергей Владимирович – проректор (по учебной и научной работе) Санкт-Петербургской академии Следственного комитета, доктор юридических наук, профессор полковник юстиции.

О В.В. Бычкове и его роли в развитии уголовно-правовых наук.

Клименко Алексей Иванович – начальник кафедры теории государства и права Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук профессор.

Средства и механизмы противодействия экстремистской идеологии.

Карагодин Валерий Николаевич – заведующий кафедрой криминалистики Екатеринбургского филиала Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева, заслуженный юрист Российской Федерации, доктор юридических наук, профессор полковник юстиции.

Основные элементы методики расследования киберпреступлений экстремистской направленности, совершаемых несовершеннолетними.

Бражников Дмитрий Анатольевич – доцент кафедры административного и таможенного права Российской таможенной академии, кандидат юридических наук, доцент, полковник полиции в отставке.

Некоторые аспекты оперативно-разыскного обеспечение раскрытия преступлений.

Оргкомитет конференции

Р.И. Бардачевский
Следственный комитет
Российской Федерации

Некоторые особенности доказывания деятельности экстремистских сообществ в сети интернет

Аннотация. В приведенной статье автор описывает и характеризует ряд некоторых криминалистических особенностей установления деятельности и связей участников экстремистских сообществ в сети интернет.

Ключевые слова: расследование деятельности экстремистских сообществ, экстремизм в сети интернет.

Интернет предоставляет экстремистским сообществам анонимность, широкую аудиторию, высокую скорость распространения информации и мультимедийные возможности, что существенно затрудняет выявление и доказывание их противоправной деятельности.

Так, экстремистские материалы могут распространяться через сайты, социальные сети, мессенджеры, форумы, видеохостинги и файлообменники, что требует комплексного подхода к сбору доказательств.

Доказывание фактов противоправных действий в интернете в большинстве случаев основывается на данных, сохранённых в цифровом виде: скриншоты, логи, метаданные, IP-адреса, переписка, публикации и мультимедийные файлы. Коллективом авторитетных авторов справедливо отмечено, что на сегодняшний день, у следствия есть несколько направлений работы с электронными следами, содержащимися в памяти сотовых телефонов, изымаемых у участников незаконных объединений:

1. Извлечение и анализ полных данных (переписка в чатах, SMS, список контактов, последние соединения, заметки, фото, видео, используемые сайты, интернет история и пр.), имеющихся в мобильном устройстве (в том числе удаленных) с помощью универсального устройства извлечения судебной информации (UFED Touch, Мобильный криминалист, XRY и др.).

2. Определение местонахождения электронного устройства (а, следовательно, и его владельца). С помощью спутниковой навигации - функции геопозиционирования (GPS/ГЛОНАСС) или соединения с точками доступа сети WiFi, а также метаданных фотоснимков, видеороликов, веб-сайтов не сложно установить координаты местоположения мобильного телефона участника уголовного судопроизводства в определенное время[1].

В свою очередь, в рамках расследования уголовных дел об экстремистских сообществах проводят экспертизы (лингвистическая, психолого-лингвистическая, культурологическая), которые играют ключевую роль в установлении экстремистского характера материалов, выявлении скрытых призывов и интерпретации смысловых нюансов.

При этом анонимность пользователей, использование VPN, прокси и подставных аккаунтов затрудняет установление личности распространителя экстремистских материалов. В данной связи для идентификации привлекаются технические средства, анализ цифровых следов, взаимодействие с администрацией интернет-платформ, международное сотрудничество.

При проведении компьютерно-технических судебных экспертиз по средствам связи участников экстремистских сообществ решают следующие задачи:

1) анализ местоположения абонента:

– классификация мест нахождения абонента (дом, работа, дача, типичное / случайное место и т.д.);

– подтверждение/опровержение нахождения абонента в интересующее время, по интересующему адресу (точность зависит от типа данных);

– маршрут передвижения абонента (привязка к карте дорог);

2) анализ собеседников абонента:

– классификация собеседников абонента (семья, работа);

– классификация собеседников по странам, городам и районам;

– выявление круга общения;

– динамика общения;

3) выявление аномалий поведения абонента:

---

[1] Тактика следственного осмотра по делам о киберпреступлениях: учебно-методическое пособие. Хатов Э.Б., Любавский А.Ю., Скобелин С.Ю. и др. М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2023. С. 35.

– география (отпуск, смена места жительства, работы, типичных маршрутов);

– плотность соединений в определенный день (поздравления с Днем рождения, профессиональным праздником, нехарактерное поведение);

– выявление смежных номеров абонента и собеседников (смена IMEI мобильного устройства, смена IMSI (индивидуальный номер абонента)): а) места, где абонент производил данные действия; б) временные характеристики, определение закономерностей; в) с кем были сеансы после смены;

4) анализ нескольких абонентов:

– определение степени корреляции между двумя и более абонентами (по собеседникам, местоположению, типам сеансов связи);

– определение совместных мест пребывания;

– общие места (дом, работа);

– визуализация одновременных маршрутов перемещения (кто куда перемещался в одно и тоже время);

5) сравнение участков местности (места абонентов):

– один абонент в разных местах;

– соединения разных абонентов между заданными местами;

– поиск смежных номеров абонентов;

– поиск абонента по шаблону поведения (настройка по классификаторам);

– выявление нетипичных абонентов для конкретного места (отсечение жителей);

6) проверка собеседников по «черным» и «белым» спискам (ранее проходившие по делам и наиболее важные контакты)[1].

Таким образом, эффективное доказывание по делам об организации и участии в экстремистских сообществах требует сочетания правовых, технических, экспертных и организационных мер, а также постоянного совершенствования методов мониторинга и анализа интернет-контента, знания возможностей судебных компьютерно-технических экспертиз.

---

[1] Сбор и анализ цифровых следов преступления: практическое пособие / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло. – СПб: Санкт-Петербургская академия Следственного комитета, 2023. С. 37–38.

Список источников

1. Сбор и анализ цифровых следов преступления: практическое пособие / С.В. Петраков, М.А. Гудкова, Д.П. Бащук, А.А. Тимофеев, Д.Н. Пигильдин, И.С. Бедеров, Д.О. Сорокин, А.В. Пытайло. СПб: Санкт-Петербургская академия Следственного комитета, 2023. – 98 с.
2. Тактика следственного осмотра по делам о киберпреступлениях: учебно-методическое пособие / Э.Б. Хатов, А.Ю. Любавский, С.Ю. Скобелин и др. М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2023. – 117 с.

С.Н. Боков[1]**, М.В. Стояновский**[2]
Воронежский государственный университет

Алгоритм психолого-криминалистического анализа материалов социальных сетей (на примере социальной сети ВКонтакте) в обеспечении расследования киберпреступлений в сфере экстремизма различного рода

Аннотация. Современный период характеризуется качественной модернизацией преступности, выражающейся, прежде всего, в распространении относительно нового феномена – киберпреступлений. Немалое количество преступлений совершается либо в социальных сетях, либо с их помощью, что влечёт за собой неизбежное оставление преступниками улик на просторах сети Интернет. Социальные сети – это не только место, где могут совершаться преступные деяния, но и прекрасный инструмент, с помощью которого соответствующие службы способны собирать ту информацию о людях, которая способствовала бы раскрытию и расследованию различных преступлений.

Ключевые слова: криминалистика; киберпреступления; экстремизм; расследование преступлений; социальные сети; криминалистическая психология.

Современный период в России характеризуется качественной модернизацией преступности, выражающейся, прежде всего, в распространении относительно нового феномена – киберпреступлений – многочисленных разновидностей преступных деяний, совершаемых с помощью компьютерных объектов (в широком смысле слова), а также в отношении этих объектов (компьютерных систем, сетей, информационных данных).

Криминальная «кибер-составляющая», на настоящий момент, является характерной особенностью ряда преступных деяний (их основных или квалифицированных составов) – от мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) до понуждения к действиям сексуального характера (п. «б» ч. 3 ст. 133 УК РФ), от доведения до самоубийства (п. «д» ч. 2 ст. 110 УК РФ) до преступлений экстремистской направленности (ст. 282 УК РФ). Это обусловливает необходимость выработки новых подходов к расследованию (и предупреждению) этих преступлений, разработки и совершенствования криминалистических методик расследования киберпреступлений, в том числе киберэкстремизма того или иного рода.

По сути, киберпреступность, с одной стороны, представляя собой относительно новый и самостоятельный криминологический феномен, в то же время не только «затрагивает» собой структуры иных известных подсистем общего феномена преступности, но и модернизирует эти подсистемы. Указанное обстоятельство, изменяющиеся условия социальной действительности, процессы обновления законодательства, «оптимизация» механизмов подготовки, совершения и сокрытия киберпреступлений, – все эти факторы обусловливают необходимость выработки, соответственно, и новых подходов к расследованию (и предупреждению) этих преступлений, разработки и совершенствования криминалистических методик расследования киберпреступлений, в т. ч., киберэкстремизма того или иного рода.

Сущность методических основ расследования таких преступлений предопределяется комплексом фундаментальных положений, практически значимых для продуктивного расследования преступлений любого вида.

Наряду с общим алгоритмом деятельности по исследованию киберпреступлений, системность и результативность этой деятельности обеспечивается использованием частных

(специальных) алгоритмов, выступающих (по отношению к общему алгоритму-системе) подсистемами криминалистической деятельности. К числу таких подсистем в алгоритме криминалистического исследования киберэкстремизма, в силу распространения данного феномена в социальных сетях, мы полагаем, относится алгоритм психолого-криминалистического анализа материалов социальных сетей.

Немалое количество преступлений в настоящее время совершается либо в социальных сетях, либо с их помощью, что влечёт за собой неизбежное оставление преступниками улик на просторах сети Интернет, в частности в социальных сетях. Социальные сети - это не только место, где могут совершаться преступные деяния, но и прекрасный инструмент, с помощью которого соответствующие службы способны собирать ту информацию о людях, которая способствовала бы раскрытию и расследованию различных преступлений.

Основным удобством социальных сетей является то, что социальные сети имеют возможность поиска необходимых контактов, а также в последствии установление связей между людьми, распространение фото- и видеоматериалов, создание групп, сообществ. Все это можно активно использовать при расследовании разных преступлений. При этом следует помнить, что информация, которая размещается в социальных сетях может быть недостоверной, поэтому следует проявлять особенную внимательность и осторожность при выборе такой информации.

Нами предлагается следующий алгоритм психологического анализа страницы в социальной сети как инструмента дистанционной психодиагностики (на примере социальной сети ВКонтакте).

1) **Сбор общей информации** (пол, возраст, образование – уровень, профиль, профессия, выполняемая в настоящее время работа, место работы, семейное положение)

На данном этапе определяется общий объем доступной информации и сама возможность проведения анализа. Основная информация является базисом для формирования портрета личности. Однако порой данная информация бывает ложной. Поэтому ее нужно сравнивать с данными из последующих этапов анализа.

2) **Работа с фотографиями**

В первую очередь стоит обратить внимание на аватар, ведь это «виртуальное лицо» человека, выбору которого уделяется больше

всего внимания. В зависимости от содержимого аватар может передавать душевное состояние человека, его цели, жизненные ценности.

При анализе фотографий на странице необходимо собрать данные по следующим параметрам: количество фото; частота публикаций; запечатлённые места/события; выражение лица; позы; одежда, аксессуары; совместные/одиночные фото; комментарии; цветность (цветные или чёрно-белые).

Если у человека много фотографий, если он часто пополняет фотоальбом, то, скорее всего, реальный мир ему не так интересен, как виртуальный. Ему/ей не хватает внимания окружающих. Значительная доля фото, содержащих различные атрибуты роскоши, говорят о том, что человек пытается доказать всем, возможно и самому себе, свою успешность и значимость, хочет, чтобы ему завидовали. Профессионально снятые и отредактированные фото, изображающие человека с лучших сторон (особенно популярны среди девушек), дают понять, что человек хочет показать себя привлечь к себе внимание. По предпочтениям в цветах можно судить об эмоциональном настрое. По фотографиям в соцсетях можно понять, какой желаемый образ человек хочет закрепить в сознании окружающих: веселого и дружелюбного, замкнутого и злого, успешного и делового или простого и свободного

3) **Анализ списка сообществ**

Данный раздел позволяет определить увлечения человека, идеологические взгляды, склад ума. По количеству сообществ можно будет судить о продолжительности посещения соцсети (где человеку интереснее: в реальном или виртуальном мире). Стоит обратить внимание на подписки, объединенные общей тематикой, а также на те сообщества, которые наиболее интересны человеку (в списке подписок они будут в самом верху). Обширная коллекция подписок позволяет определить личностные качества.

4) **Работа с музыкальной коллекцией**

На этом этапе необходимо ознакомиться с персональной аудио коллекцией. Стоит обратить внимание на количество треков. Обширная аудио коллекция – характерная черта меломана. Также важно определить любимый музыкальный жанр. Отсортировав список аудиозаписей по дате добавления, можно определить в каком эмоциональном состоянии находился человек в последнее время.

5) **Работа с записями на стене**

Просмотрев записи на стене, можно собрать много информации. Записи на своей странице люди могут сохранять по разным причинам, но всех их объединяет желание поделиться интересным контентом. Творческие люди любят сохранять на стене свои работы, чтобы их оценили. На стене в соцсети могут быть записи на любую тему: посвященные любимому делу, хобби, месту, которое человек хотел бы посетить, моде, спорту, уходу за питомцами, рецепты, фильмы и сериалы, статьи и книги, цитаты философов, а также юмористический контент. По записям, соответственно, тоже можно определить личные увлечения.

6) Работа со списком друзей

При работе с данным разделом стоит уделить внимание количеству друзей. Много друзей в соцсети у человека может быть по ряду причин. Это может быть попытка раскрутить свой сайт, интернет-магазин, заработать на рекламе. Много подписчиков может быть у блогера, талантливого творческого человека. Бывают ситуации, когда люди специально набирают много друзей, чтобы чувствовать себя крутыми и популярными. Однако это и может быть одинокий человек, которому хочется новых знакомств, общения и впечатлений. В обратной ситуации, когда очень мало друзей или их вообще нет, можно говорить о замкнутости человека. При этом важно учесть, как давно создана страница.

Объединив эти данные с информацией, полученной на втором этапе («лайки» и комментарии), можно определить: с кем чаще взаимодействует человек; в каких взаимоотношениях находится; какое положение занимает среди друзей.

7) **Работа с видео**

Данный этап идентичен третьему. Однако он является дополнительным. Этому послужило уменьшение интереса у людей к формированию собственной коллекции видеозаписей в социальных сетях. По коллекции видео можно узнать о личных интересах и увлечениях. По большой коллекции фильмов и сериалов можно определить инфантильного человека. Предпочтения в жанрах позволяют определить черты характера.

Выводы

На данном этапе обобщается вся полученная информация.

Таким образом, можно сделать вывод о том, что изучение страницы в социальной сети играет большую роль в получении

криминалистической информации о личности преступника, в частности его индивидуально-психологических особенностях. Внимательно изучая информацию из социальной сети, можно получить много необходимых данных о преступнике и его действиях.

Д.В. Бражников
Российская таможенная академия

Некоторые аспекты оперативно-разыскного обеспечение раскрытия преступлений

Оперативно-разыскное обеспечение раскрытия преступлений является одним из элементов организационно-тактических форм оперативно-разыскной деятельности (далее – ОРД) и должно осуществляться еще до возбуждения уголовного дела, поскольку «именно с оперативно-разыскной деятельности чаще всего начинается работа по раскрытию преступлений. Она по времени ближе к моменту обнаружения преступления, в идеале ведется по горячим следам»[1]. Данное положение отражается в статье 11 Федерального закона № 144-ФЗ «Об оперативно-разыскной деятельности», что результаты ОРД могут служить поводом и основанием для возбуждения уголовного дела, использоваться в доказывании по уголовным делам в соответствии с законодательством РФ.

В общем виде систему оперативно-разыскного обеспечения раскрытия преступлений можно представить в следующем виде:

1. Теоретические основы обеспечения рассматриваемой сферы деятельности, в том числе их совершенствование, адаптация отечественного законодательства и правоприменительной практики к положительному опыту зарубежных стран, неукоснительное соблюдение правоохранительными органами требований нормативных актов – как основные меры обеспечения общественной безопасности РФ[2].

---

[1] Оперативно-разыскная деятельность: учебник. 2-е изд., доп. и перераб. / под ред. К.К. Горяинова. М.: ИНФРА-М, 2004. XIV. 848 с.

[2] Концепция общественной безопасности в Российской Федерации (утв. Президентом РФ 14.11.2013 № Пр-2685).

2. Материально-техническое обеспечение, которое в рассматриваемой сфере преступности особенно ценно для их качественного раскрытия – специальная техника, информационные устройства, информационно-поисковые системы, оперативно-разыскные и иные учеты, базы данных и т.д.

3. Организационное обеспечение, то есть непосредственная практическая реализация мер, регламентирующая основания и условия проведения оперативно-разыскных мероприятий (далее – ОРМ), документирование преступной деятельности и использование результатов ОРД в доказывании по уголовным делам. Организационное обеспечение предусматривает осуществление комплекса ОРМ, направленных на документирование преступной деятельности лиц, например от подозреваемого лица к совершаемому им преступлению и от совершенного преступления к подозреваемому.

Очевидно, что в основном такие меры сводятся в основном к негласному характеру ОРД, что отражает специфику ее деятельности. По причине высокой латентности преступлений чаще всего раскрытие таких преступлений реализуется по организационно-тактической схеме от преступления – к лицу, его совершившему1.

После совершенного преступления наступает важный этап оперативной работы по проверке оперативной информации – оценка, анализ и выдвижение оперативно-разыскных версий. Затем планируются комплекс необходимые ОРМ и тактических действий, с учетом оперативной обстановки в целях подтверждения или опровержения факта преступления. Здесь важно установить очередность и тактику их проведения, определить перечень необходимых сил, средств и методов, которые при этом целесообразно использовать.

Реализация полученной информации при проведении ОРМ для раскрытия преступлений происходит в рамках документирования.

В целях признания оперативно-разыскной информации о преступлениях доказательствами, можно придерживаться следующих «правил»:

– проводить ОРМ, направленные на документирование преступной деятельности, по возможности, таким образом, чтобы исключить

[1] Основы оперативно-разыскной деятельности: учебное пособие / В.В. Бычков, Д.А. Бражников и др. М.: Юнити-Дана, 2021. 207 с.

участие в них конфидентов, привлекать к ним строго ограниченный круг участников;

– обеспечить возможность и готовность сотрудников, участвующих в ОРМ, быть допрошенными в качестве свидетелей;

– при планировании и осуществлении ОРМ необходимо обеспечить выполнение всех требований законодательства, обратив внимание на положения, регламентирующие правомочия должностных лиц и особенности проведения каждого конкретного ОРМ.

Однако, как отмечают специалисты, качественный уровень оперативно-разыскного обеспечения раскрытия преступлений можно достичь посредством «стандартизации процесса получения, обработки, преобразования, реализации и использования оперативной информации в рамках уголовно-процессуального доказывания»[1]. Актуальность проблематики связана с тем, что при большом значении результатов ОРД для установления обстоятельств, входящих в предмет доказывания, действующее оперативно-разыскное и уголовно-процессуальное законодательство не позволяет их рассматривать как доказательства. Результаты ОРД являются лишь «сведениями об источниках тех фактов, которые могут стать в последующим доказательствами, только после закрепления их надлежащим процессуальным путем, а именно – на основе соответствующих норм уголовно процессуального закона.

Таким образом, процесс оперативно-разыскного обеспечения раскрытия преступлений представляет собой комплекс мер, реализуемых оперативными подразделениями с применением сил, средств и методов ОРД в целях создания условий для эффективного обеспечения процесса доказывания, пресечения преступлений, неотвратимости наказания лиц, виновных в совершении преступлений.

[1] Иванов П.И. О разработке отечественной системы оперативно-розыскного обеспечения экономической безопасности социально-бюджетной сферы / П.И. Иванов // Труды Академии управления МВД России. 2019. № 3 (51). С. 61.

Е.Г. Быкова
Московская академии Следственного комитета
имени А.Я. Сухарева

О признаке публичности призывов к террористической или экстремистской деятельности, размещенных в информационно-телекоммуникационных сетях

Аннотация. В статье исследуется проблема квалификации преступлений, предусмотренных ч. 2 ст. 205.2 УК РФ и ч. 2 ст. 280 УК РФ, в случае адресации призывов ограниченному кругу лиц. По результатам анализа теоретических положений и судебной практики резюмировано наличие признака публичности. Предложено дополнить соответствующими разъяснениями п. 4 Постановления Пленума Верховного Суда РФ от 28.06.2011 № 11 и п. 19 Постановления Пленума Верховного Суда РФ от 09.02.2012 № 1.

Ключевые слова: экстремизм, терроризм, публичные призывы, информационно-телекоммуникационные сети, киберпреступление.

Председатель Следственного комитета Российской Федерации А.И. Бастрыкин констатирует, что в настоящее время происходит увеличение роста числа преступлений, совершенных с использованием информационно-телекоммуникационных сетей, и в среднесрочном периоде эта тенденция будет сохраняться[1]. С точки зрения А.А. Бессонова количественный рост киберпреступности напрямую зависит от всеобъемлющего распространения информационно-телекоммуникационных технологий[2].

В.В. Бычков отмечал, что Интернет и мобильная телефония все шире используются при совершении преступлений экстремистской направленности, в частности, публичных призывов к осуществлению

[1] Бастрыкин А.И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 89.

[2] Бессонов А.А. Киберпреступность: тенденции и перспективы // Расследование преступлений: проблемы и пути их решения. 2024. № 3(45). С. 24.

экстремистской деятельности[1], ответственность за которые предусмотрена в ч. 2 ст. 280 Уголовного кодекса РФ[2] (далее – УК РФ). Его наблюдения подтверждаются статистическими данными Министерства внутренних дел РФ. Так, за январь-декабрь 2024 года зарегистрировано 447 преступлений, предусмотренных ч. 2 ст. 280 УК РФ (на 21,8 % больше, чем за аналогичный период 2023 года). Следует отметить, что они успешно расследуются правоохранительными органами. За указанный период в суд направлено 372 уголовных дела (на 5,4 % больше, чем за аналогичный период 2023 года)[3].

Одним из факторов, влияющих на положительный результат работы, является правильное применение уголовного закона. При оценке публичных призывов к осуществлению экстремистской деятельности могут возникать сложности установления предусмотренных в ч. 1 ст. 280 УК РФ признаков. Так, при совершении таких призывов с использованием информационно-телекоммуникационных сетей не всегда однозначно решается вопрос о наличии обязательного признака – публичности. Аналогичная проблема существует при квалификации публичных призывов к осуществлению террористической деятельности, ответственность за которые предусмотрена в ч. 2 ст. 205.2 УК РФ[4,5].

---

[1] Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 28.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС КонсультантПлюс.

[3] Официальный сайт Министерства внутренних дел Российской Федерации. Состояние преступности в России за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 02.04.2025).

[4] В соответствии с пп. «а» п. 1 ч. 1 ст. 151 Уголовно-процессуального кодекса РФ это преступление относится к подследственности следователей Следственного комитета РФ.

[5] За январь-декабрь 2024 года зарегистрировано 898 преступлений, предусмотренных ч. 2 ст. 205.2 УК РФ (на 69,3 % больше, чем за аналогичный период 2023 года), в суд направлено 573 уголовных дела. См. официальный сайт Министерства внутренних дел РФ. Состояние преступности в России за январь-декабрь 2024 года. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 02.04.2025).

Публичность является оценочным признаком. Для его установления нужно учитывать место, способ, обстановку и другие обстоятельства дела. Высшая судебная инстанция в качестве примеров приводит, в частности, обращения к группе людей в общественных местах, на собраниях, распространение обращений путем массовой рассылки сообщений абонентам мобильной связи[1]. В.В. Бычков отмечал, что «публичность характеризует внешнее окружение, в условиях которого совершаются призывы, и понимается как открытость, доступность, способность быть воспринимаемыми неопределенным кругом лиц», количество присутствующих или воспринявших призывы не имеет решающего значения[2].

Сомнений в публичности призывов к осуществлению экстремистской или террористической деятельности не возникает, если они размещены в открытом доступе в информационно-телекоммуникационной сети, включая сеть Интернет, и ознакомиться с ними может любой человек[3].

Однако наличие квалифицирующего признака, предусмотренного частями вторыми ст. 205.2 УК РФ и ст. 280 УК РФ, не зависит от количества компьютерных устройств, входящих в такую технологическую систему, подключения к ней ограниченного количества пользователей или неопределенного круга лиц[4]. В этой связи представляет сложность оценка призывов как публичных в ситуациях, когда они размещены в ограниченном доступе, например,

---

[1] П. 4 Постановления Пленума Верховного Суда РФ от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», п. 19 Постановления Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // СПС КонсультантПлюс.

[2] Противодействие преступлениям экстремистской направленности: курс лекций / В.В. Бычков. М.: Юрлитинформ, 2013. С. 90–91.

[3] См., например, кассационные определения Судебной коллегии по делам военнослужащих Верховного Суда РФ от 22.03.2023 № 223-УД23-4-А6, от 06.02.2024 № 223-УД24-1-А6, от 15.10.2024 № 224-УД24-56-А6, от 05.12.2024 № 225-УД24-25-А6 // СПС КонсультантПлюс».

[4] П. 17 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» // СПС КонсультантПлюс.

на закрытой странице в социальной сети, на компьютерном устройстве, подключенном к локальной сети, в групповом чате в мессенджере. В теории уголовного права четкого ответа на этот вопрос нет.

С.В. Борисов и А.В. Жеребченко полагают, что минимальный порог количества лиц, образующий публику и публичность, – два человека. Они считают, что применительно к преступлениям, совершенным с использованием информационно-телекоммуникационных сетей, признак публичности характеризуется доступностью используемой информации для понимания широкого круга людей[1].

Д.А. Бажин также предлагает понимать под публичностью обращение к двум и более лицам. При этом он справедливо указывает на несинонимичность понятий «широкий круг лиц» и «неопределенный круг лиц» и задается вопросами «для кого именно этот круг лиц должен быть неопределенным и как поступать в том случае, если численность этих лиц была велика и доподлинно известна субъекту преступления?»[2].

Ответить на эти вопросы затруднительно. Развивая мысль Д.А. Бажина, возможно лишь задать дополнительные. В частности, остается неясным, имеется ли признак публичности в случае совершения призывов к экстремисткой или террористической деятельности в созданном студентами учебного заведения для общения по вопросам обучения групповом чате в мессенджере. Такое сообщество по своей сути представляет собой собрание. Количество и круг лиц ограничены. Это могут быть студенты одной учебной группы или одного курса. Представляется, что нужно учитывать один нюанс – участники группового чата объединились для обсуждения вопросов, не связанных с экстремистской или террористической деятельностью, и вряд ли положительно отреагируют на адресованные им призывы. Думается, что в обозначенной ситуации признак публичности наличествует независимо от количества участников.

---

[1] Борисов С.В., Жеребченко А.В. Возбуждение ненависти, вражды, унижение человеческого достоинства: проблемы установления и реализации уголовной ответственности. Монография / Отв. ред. С.В. Борисов. М.: Юриспруденция, 2015. Доступ из СПС КонсультантПлюс.

[2] Бажин Д.А. К вопросу о понимании публичности в уголовном праве // Российский юридический журнал. 2011. № 2. Доступ из СПС КонсультантПлюс.

О.В. Костылева применительно к ст. 282 УК РФ высказывает мнение о возможности признания деяния малозначительным, при условии, что потенциальное количество адресатов небольшое (немногочисленные «друзья» в социальной сети), отсутствует значительное количество просмотров, а ознакомившиеся с опубликованным «ненавистническим» материалом не проявили свою заинтересованность в поддержании взглядов автора или тем более выразили свой протест идеям адресанта[1].

Учитывая, что призывы представляют собой побуждение иных лиц к исполнению запрещенных законом деяний, возможность применения ч. 2 ст. 14 УК РФ при схожих обстоятельствах видится дискуссионной. Их общественная опасность велика, поэтому преступления, предусмотренные ст. 205.2 УК РФ и ст. 280 УК РФ, окончены с момента совершения призывов независимо от результатов такого побуждения[2].

С учетом изложенного представляется, что признак публичности наличествует при совершении с использованием информационно-телекоммуникационных сетей призывов к осуществлению террористической или экстремисткой деятельности, обращенных к ограниченному кругу лиц. Решению этой правоприменительной проблемы может способствовать дополнение соответствующими разъяснениями п. 4 Постановления Пленума Верховного Суда РФ от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» и п. 19 Постановления Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

---

[1] Костылева О.В. Уголовная ответственность за возбуждение ненависти или вражды: новые разъяснения Пленума Верховного Суда РФ и международные стандарты в области прав человека // Уголовное право. 2018. № 6. Доступ из СПС КонсультантПлюс.

[2] П. 4 Постановления Пленума Верховного Суда РФ от 28.06.2011 № 11«О судебной практике по уголовным делам о преступлениях экстремистской направленности», п. 20 Постановления Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // СПС КонсультантПлюс.

Список источников

1. Бажин Д.А. К вопросу о понимании публичности в уголовном праве // Российский юридический журнал. 2011. № 2. С. 162–168.

2. Бастрыкин А.И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 88–94.

3. Бессонов А.А. Киберпреступность: тенденции и перспективы // Расследование преступлений: проблемы и пути их решения. 2024. № 3(45). С. 23–30.

4. Борисов С.В., Жеребченко А.В. Возбуждение ненависти, вражды, унижение человеческого достоинства: проблемы установления и реализации уголовной ответственности. Монография / Отв. ред. С.В. Борисов. М.: Юриспруденция, 2015. 264 с.

5. Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 26–31.

6. Костылева О.В. Уголовная ответственность за возбуждение ненависти или вражды: новые разъяснения Пленума Верховного Суда РФ и международные стандарты в области прав человека // Уголовное право. 2018. № 6. С. 66–80.

7. Бычков В.В. Противодействие преступлениям экстремистской направленности: курс лекций. М.: Юрлитинформ, 2013. 256 с.

Е.И. Бычкова
Московская академия Следственного комитета
имени А.Я. Сухарева

Концепция совершенствования полномочий органов местного самоуправления в сфере профилактики терроризма и экстремизма

Аннотация. В статье анализируются полномочия органов местного самоуправления в сфере профилактики терроризма и экстремизма, нормативно-правовая основа противодействия на уровне местного самоуправления. Обосновывается необходимость выработки эффективных мер, направленных на профилактику терроризма и экстремизма, предлагается концепция совершенствования полномочий органов местного самоуправления в рассматриваемой сфере.

Ключевые слова: местное самоуправление, профилактика терроризма и экстремизма, муниципальная программа

Согласно статье 32 Федерального закона от 20.03.2025 № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти», который вступает в силу с 19 июня 2025 года к полномочиям органов местного самоуправления по решению вопросов непосредственного обеспечения жизнедеятельности населения относится участие в профилактике терроризма и экстремизма, а также в минимизации и (или) ликвидации последствий проявлений терроризма и экстремизма в границах муниципального образования.

Правовую основу участия муниципальных образований в профилактике терроризма и экстремизма составляют Стратегия национальной безопасности Российской Федерации, утверждённая Указом Президента РФ от 2 июля 2021 года № 400, Стратегия противодействия экстремизму в Российской Федерации, утвержденная Указом Президента России от 28 декабря 2024 г. № 1124, Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных

технологиях и о защите информации», Концепция противодействия терроризму в Российской Федерации, Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» и иные нормативные правовые акты, законы субъектов Российской Федерации, а также муниципальные правовые акты и муниципальные программы, утверждаемые представительными органами муниципальных образований.

Учитывая, что указанные преступления представляют угрозу всему государству в целом, подрывают основы конституционного строя, посягают на общественную безопасность, обладают повышенной социальной опасностью, то компетенция органов местного самоуправления в этой сфере не значительна, поскольку основная масса решений, принимаемых мер, направленных на профилактику терроризма и экстремизма, остается за органами государственной власти.

Тем не менее именно местное самоуправление является самым приближенным к населению уровнем публичной власти, через которые и реализуется государственная политика по профилактике терроризма и экстремизма. Так, например, органы местного самоуправления осуществляют непосредственно охрану общественного порядка, в ходе которой могут выявляться преступления, о которых идет речь. Однако этого недостаточно. На муниципальном уровне механизм профилактики терроризма и экстремизма еще недостаточно отработан и проработан с научной и правовой точки зрения, вопрос о том, что конкретно входит в понятие «участие в профилактике» и где данное участие начинается и заканчивается остается открытым.

Красочные плакаты «Внимание терроризм!», размещаемые в общественных местах, организациях, учреждениях не оказывают должного профилактического эффекта, поскольку уже не привлекают к себе внимание, тем более молодежи. А важной составляющей профилактики являются меры пропагандистского и воспитательного характера, когда жители муниципального образования, обладая должным правосознанием будут проявлять активность, уведомлять органы власти, правоохранительные органы о проявлении террористического или экстремистского поведения. Именно на население делаются ставки в вопросе выявления подобных преступлений на стадии их подготовки, а население, в свою очередь, должно обладать соответствующими навыками и умениями

различать предпосылки возможного преступного поведения. С этой целью в муниципальных учреждениях, предприятиях, организациях необходимо регулярно осуществлять просветительскую работу, направленную на выработку навыков у населения выявлять потенциальную угрозу, противостоять ей. Особое внимание в этом направлении обратить на образовательные учреждения, педагогов и обучающихся. Именно несовершеннолетние граждане становятся чаще всего вовлеченными в деструктивную идеологию терроризма и экстремизма и максимально подвержены ее воздействию.

Кроме того, представляется, что органам местного самоуправления необходимо на регулярной основе осуществлять взаимодействие с правоохранительными органами, полномочия которых в вопросах борьбы с терроризмом и экстремизмом наиболее широкие (например, проводить оперативно-разыскные мероприятия). Необходимо осуществлять совместное проведение совещаний, организовывать научно-практические форумы, посвященные профилактике и совместными усилиями выработать наиболее оптимальные для конкретного муниципального образования меры по профилактике рассматриваемых преступлений[1].

Требуется согласованное планирование мероприятий в сфере противодействия терроризму и экстремизму, их координация и правовое обеспечение.

Итак, концепция совершенствования полномочий органов местного самоуправления по участию в профилактике терроризма и экстремизма на территории муниципального образования включает в себя следующие элементы:

- принятие муниципальных программ профилактики терроризма и экстремизма, предупреждения межнациональных (межэтнических) конфликтов, в которых подробно отражать мероприятия профилактического характера. Разработка программ должна производиться при непосредственном участии правоохранительных органов (сотрудников прокуратуры, МВД, ФСБ, Следственного комитета);

- механизм реализации муниципальных программ профилактики терроризма и экстремизма должен предусматривать формирование

[1] Бычкова Е.И., Бычков В.В. Участие органов местного самоуправления в противодействии экстремизму: концептуальные основы и проблемы реализации // Расследование преступлений: проблемы и пути их решения. 2021. № 2(32). С. 36.

объективного ресурсного обеспечения и расходных обязательств муниципального образования на обеспечение мер профилактики;

- при формировании документов стратегического планирования и муниципальных программ профилактики терроризма и экстремизма проводить консультации с общественными объединениями, представителями молодежных организаций и иными институтами гражданского общества;

- организовывать конкурсы на территории муниципального образования на лучший инициативный проект по профилактики терроризма и экстремизма;

- всестороннее в СМИ, на Интернет-ресурсах освещать меры, принимаемые на территории муниципального образования, направленные на реализацию государственной политики в сфере борьбы с терроризмом и экстремизмом, а также гармонизации межнациональных (межэтнических) и межконфессиональных отношений, а также в целях снижения уровня ксенофобии;

- осуществлять широкую поддержку организациям, осуществляющим просветительскую работу в сфере профилактики преступлений;

- в муниципальные программы развития образования включать меры по воспитанию у подрастающего поколения уважительного отношения к национальностям и конфессиям, а также по обучению действиям в момент угрозы террористического акта и разъяснению преступной сущности преступлений террористической и экстремистской направленности;

- осуществлять регулярный мониторинг в образовательных организациях, направленный на выявление в среде молодежи фактов распространения материалов и идей террористического или экстремистского характера;

- создать систему гражданского контроля на предмет выявления материалов террористического или экстремистского характера в сети Интернет и иных источниках СМИ и передачи информации в правоохранительные органы[1].

[1] Дондоков Г.Р., Дондоков Ц.С. О некоторых проблемах, стоящих перед органами местного самоуправления в сфере профилактики терроризма и экстремизма среди молодежи // Государственная власть и местное самоуправление. 2020. № 8. С. 47–50.

Список источников

1. Бычкова Е.И., Бычков В.В. Участие органов местного самоуправления в противодействии экстремизму: концептуальные основы и проблемы реализации // Расследование преступлений: проблемы и пути их решения. 2021. № 2(32). С. 36.
2. Дондоков Г.Р., Дондоков Ц.С. О некоторых проблемах, стоящих перед органами местного самоуправления в сфере профилактики терроризма и экстремизма среди молодежи // Государственная власть и местное самоуправление. 2020. № 8. С. 47–50.

В.Ф. Васюков
Московская академия Следственного комитета
имени А.Я. Сухарева

Природа и роль цифровой информации в расследовании преступлений

Аннотация. В статье рассматривается понятие цифровой информации в контексте его использования при расследовании уголовных дел. Автор анализирует различные подходы к определению информации, выделяя ключевые концепции – коммуникативную, атрибутивную и функциональную. На основе анализа доктринальных источников и норм уголовно-процессуального права предложено уточнённое понимание цифровой информации, способствующее её более эффективному использованию в расследовании преступлений.

Ключевые слова: цифровая информация, доказывание, уголовное дело, электронный носитель, расследование.

В современном обществе наблюдается стремительное развитие цифровых технологий, которые оказывают значительное влияние на все сферы жизнедеятельности, в том числе на уголовное судопроизводство. В условиях роста числа мошеннических действий с использованием информационно-коммуникационных технологий

цифровая информация приобретает решающее значение для раскрытия и расследования преступлений[1].

Однако эффективное использование цифровой информации в уголовном судопроизводстве затруднено из-за отсутствия четких определений и единого понимания ключевых понятий и терминов, относящихся к цифровой среде. В связи с этим любая научная дисциплина, стремящаяся к формированию устойчивой теоретической базы, нуждается в разработке строгого понятийного аппарата. Эмпирический опыт свидетельствует о том, что корректное определение понятий является основой для проведения углубленных исследований, обеспечивая тем самым их практическую значимость и возможность применения полученных результатов в правоприменительной практике.

Иногда смысл используемой терминологии в рамках определённого научного направления кажется очевидным, однако при более глубоком анализе исследователь может усомниться в корректности употребления тех или иных слов и их сочетаний. Например, в криминалистической теории часто встречается термин «информация». При этом он не является специфическим для криминалистики, а заимствован из других областей знаний.

Хотя этот термин кажется простым и понятным, критический анализ его применения может вызвать у исследователя неоднозначную реакцию. Это связано с разными подходами к пониманию сущности информации.

В русском языке слово «информация» определяется как: «1. Сведения об окружающем мире и протекающих в нём процессах, воспринимаемые человеком или специальным устройством. 2. Сообщения, осведомляющие о положении дел, о состоянии чего-нибудь»[2]. В контексте научной интерпретации наиболее широкое толкование информации, по нашему мнению, представлено в философских исследованиях. При этом, несмотря на кажущуюся очевидность этого понятия, его глубина, форма и содержание постоянно меняются в зависимости от прогресса научного знания.

В современной философской мысли проблема сущности информации остается одной из наиболее дискуссионных, что

---

[1] Васюков В.Ф., Дамирчиев Э.И.О. Понятие и виды цифровой информации, используемой в доказывании по уголовным делам // Криминалистика: вчера, сегодня, завтра. 2025. № 2 (34). С. 38–50.

[2] Ожегов С.И. Словарь русского языка. М., 1978. С. 242.

обусловлено как многогранностью самого феномена, так и его принципиальной значимостью для различных областей научного знания. В рамках философского анализа сформировались три ключевые концепции, раскрывающие природу информации: коммуникативная, атрибутивная и функциональная. Каждая из них акцентирует определенный аспект информационных процессов, что позволяет рассматривать их в диалектическом единстве, обеспечивающем более полное понимание данного феномена[1].

Коммуникативная концепция интерпретирует информацию в контексте общения и общенаучной рефлексии, подчеркивая ее социально-семиотическую природу. В рамках данного подхода информация трактуется как продукт знаковых систем, возникающий в процессе взаимодействия между субъектами или между субъектом и окружающей средой. Такой взгляд восходит к идеям семиотики и теории коммуникации, где информация рассматривается как сообщение, передаваемое посредством языка или иных символических структур[2]. Важным аспектом здесь является интенциональность информационного процесса: информация существует лишь в той мере, в какой она воспринимается и интерпретируется реципиентом. Следовательно, коммуникативная концепция актуализирует проблему понимания, кодирования и декодирования сообщений, что особенно значимо для гуманитарных наук, изучающих социальные взаимодействия[3].

В противоположность этому, *атрибутивная* концепция исходит из онтологического статуса информации, трактуя ее как неотъемлемое свойство материи. Данный подход основывается на представлении о том, что информационные процессы присущи всем уровням организации материального мира — от физических взаимодействий до биологических и социальных систем. В рамках этой парадигмы информация понимается как объективная характеристика любых материальных объектов, отражающая их структуру, состояние и

---

[1] Цветков В.Я. Введение в теорию информации. Москва: ООО МАКС Пресс, 2007. 116 с.

[2] Саттарова Н.И. Информация как коммуникация // Современное образование: содержание, технологии, качество. 2013. Т. 2. С. 7–8.

[3] Мельситов В.В. Информация, коммуникация, трансляция / В. В. Мельситов, Н.Л. Сергиенко, З.К. Лакербай // Научные труды КубГТУ. 2017. № 6. С. 205–212.

взаимосвязи[1]. Так, в кибернетике и синергетике информация рассматривается как мера упорядоченности системы, а в физике — как параметр, связанный с энтропией и энергией. Атрибутивная концепция, таким образом, снимает антропоцентрический ограничитель, характерный для коммуникативного подхода, и расширяет понятие информации до универсального атрибута бытия.

Между тем, *функциональная концепция* занимает промежуточное положение между коммуникативным и атрибутивным подходами, связывая информацию исключительно с функционированием самоорганизующихся систем. В данном случае информация понимается как механизм управления и регуляции, обеспечивающий адаптацию и целенаправленное поведение систем. Функциональный подход акцентирует прагматический аспект информации: ее ценность определяется не столько семантическим содержанием, сколько эффективностью воздействия на систему. Таким образом, информация здесь выступает как инструмент управления, что особенно значимо для исследования биологических, технических и социальных систем, обладающих механизмами саморегуляции[2].

В основе современного понимания информации как научной категории лежит фундаментальный вклад К. Шеннона, который в рамках теории связи предложил строгое математическое определение информации, интерпретируя ее как меру уменьшения неопределенности. Данный подход, изложенный в работе «Математическая теория связи» (1948), не только заложил основы информатики и теории кодирования, но и оказал существенное влияние на развитие кибернетики, статистической физики и даже философии как науки. Сущность шенноновской концепции заключается в вероятностной трактовке информации: чем менее вероятно событие, тем больше информации несет сообщение о его наступлении. Эта идея, выраженная через формализм энтропии, устанавливает прямую связь между информационными процессами и статистическими закономерностями, что позволяет рассматривать

[1] Макальский, Л. М. Информационная экология / Л. М. Макальский, А. К. Макаров, О. М. Цеханович; Под ред. Л.М. Макальского. М.: ОнтоПринт, 2017. 48 с.

[2] Соколов А.В. Философия информации: Учебное пособие. – 3-е изд. – Москва: Юрайт, 2020. 175 с.

информацию как объективную величину, независимую от семантического содержания сообщений[1].

Прагматическая значимость концепции проявляется в ее приложениях к задачам передачи данных. Теорема о пропускной способности канала связи утверждает, что при скорости генерации информации, не превышающей пропускную способность, возможно сколь угодно точное кодирование сообщений даже в присутствии шумов. Это достигается за счет введения избыточности, которая компенсирует искажения, и демонстрирует, как уменьшение неопределенности (энтропии) на приемной стороне обеспечивает надежную коммуникацию[2]. Противники этого подхода указывали на его ограниченность: теория абстрагируется от смысловой и прагматической ценности информации, фокусируясь лишь на ее статистических аспектах[3]. Однако именно эта абстракция позволила создать универсальный математический аппарат, применимый как к техническим системам (сжатие данных, криптография), так и к естественнонаучным дисциплинам.

Теория К. Шеннона в дальнейшем оказала значительное влияние на исследования Н. Винера, который предложил идею о том, что информация интерпретируется не как статичный объект или абстрактная сущность, а как динамический элемент, циркулирующий в контурах обратной связи и обеспечивающий адаптацию, регуляцию и целеполагание системы[4]. Такой взгляд радикально трансформировал традиционные представления о природе информации, сместив акцент с ее семантического или субстанционального аспекта на функционально-прагматический[5].

Центральным понятием в теории Н. Винера является обратная связь, механизм которой позволяет системе корректировать свое

---

[1] Маховиков А. Е. Информация в информационном обществе: проблема определения понятия // Наука XXI века: актуальные направления развития. 2020. № 1–2. С. 294–299.

[2] Курилкина, В. Н. Философский и общенаучный анализ понятия информации / В. Н. Курилкина // Вестник Северо-Восточного федерального университета им. М.К. Аммосова. 2014. Т. 11, № 1. С. 73–77.

[3] Духин, А.А. Теория информации : учебное пособие. Москва: Московский институт электроники и математики НИУ ВШЭ, 2005. 247 с.

[4] Schetzen, M. (2005) Nonlinear system modeling based on the Wiener theory. *Proceedings of the IEEE,* vol. 69, no. 12, pp. С. 1557-1573.

[5] Медведев Д.С. Категория истины в феномене "информация" // Журнал философских исследований. 2018. Т. 4, № 4. С. 41–45.

поведение на основе поступающих данных о результатах предыдущих действий. В этом контексте информация приобретает значение не просто как передаваемое сообщение, а как содержательный компонент сигнала, который способен изменять состояние системы. Например, в технических системах управляющий сигнал, поступающий от датчиков, содержит информацию о текущих параметрах работы устройства, что позволяет регулятору вносить коррективы для достижения заданного режима[1]. Аналогичные процессы наблюдаются в биологических системах, где нервные импульсы или гормональные сигналы выполняют функцию носителей информации, обеспечивающей гомеостаз и адаптивное поведение организма.

Важным аспектом кибернетической трактовки информации является ее вероятностно-статистическая природа. Это означает, что информационная ценность сигнала определяется не только его содержанием, но и степенью неожиданности для получателя. Например, в системе автоматического регулирования аномальные показания датчика несут больше информации, чем стандартные, поскольку требуют более значимых корректирующих воздействий. Данный подход позволил формализовать понятие информации, введя количественные методы ее оценки, что стало основой для развития теории управления и компьютерных наук[2].

Кроме того, Н. Винер расширил понимание информации за пределы технических систем, распространив его на биологические и социальные процессы. В работе «Кибернетика, или управление и связь в животном и машине» он обосновал универсальность информационных механизмов, показав, что принципы обратной связи и управления лежат в основе функционирования живых организмов, экономических структур и даже культурных явлений. Так, рефлексы в нервной системе, рыночные механизмы в экономике или процессы общественной коммуникации могут быть описаны в терминах передачи и обработки информации[3].

Однако кибернетическая концепция не лишена ограничений. Критики отмечают, что сведение информации к сигналам управления

---

[1] Valentinov, V. (2017) Wiener and Luhmann on feedback: From complexity to sustainability. *Kybernetes*, vol. 46, no. 3, pp. 386–399.

[2] Хромов Л.И. Теория информации и теория познания. СПб: Русское филос. общество, 2006. 200 с.

[3] Цветков В.Я. Введение в теорию информации. М.: МАКС Пресс, 2007. 116 с.

игнорирует ее смысловую и ценностную составляющую, которая играет ключевую роль в социальных и гуманитарных контекстах[1].

Несмотря на кажущуюся противоречивость, указанные концепции не исключают, а взаимодополняют друг друга, раскрывая различные грани информационных процессов. Коммуникативный подход актуален для анализа социальных и культурных феноменов, атрибутивный — для философско-онтологических исследований, а функциональный — для изучения динамических систем. Интеграция этих концепций позволяет сформировать более целостное представление о информации как о сложном, многомерном явлении, играющем ключевую роль как в природных, так и в социальных процессах[2].

На лексическом уровне термин «цифровой» (от лат. *digitus* — палец), используемый в электронной и компьютерной сфере как антоним понятию «аналоговый», отражает технологию преобразования информации в числовую форму. Этимологическая связь с пальцами рук указывает на исторический способ счета, что объясняет использование данного прилагательного для обозначения процесса кодирования информации, преимущественно посредством бинарного кода. Последний позволяет воспроизводить данные на языке вычислительной техники через комбинацию двух значений (0 и 1).

Указанное понятие охватывает не только устройства, оперирующие числовыми величинами, но и содержащиеся в них данные с их репрезентациями. Общепринято, что данный термин применяется не только к аппаратным средствам, но и к обрабатываемой ими информации. Однако, в доктринальных источниках прослеживается терминологический плюрализм: доказательства, источником которых стала цифровая информация, обозначаются различными, зачастую взаимозаменяемыми формулировками, не всегда адекватно отражающими их природу и специфику. В условиях отсутствия законодательного закрепления формирование дефиниции

---

[1] Подгорекци Ю. Смысловое значение понятия «информация» в коммуникативных процессах / Ю. Подгорекци, Н.А. Некрасова, С.И. Некрасов // Позиция. Философские проблемы науки, техники и образования. 2012. № 5. С. 198–209.

[2] Кремлев М.В. К вопросу о понятии информации, используемой в ходе расследования преступлений // Человек: преступление и наказание. 2014. № 4(87). С. 101–104.

«электронное доказательство» представляет собой значительную методологическую сложность ввиду отсутствия легального определения данного понятия в действующем законодательстве. Несмотря на активное использование указанного термина в научных публикациях, в российской правовой системе он встречается только в контексте сопоставления с иными терминами.

Так, рассмотрев соотношение понятий «цифровая информация» и «электронное доказательство», Н.В. Олиндер, приходит к выводу о некорректности использования термина «электронное доказательство». Основной аргумент состоит в том, что информация, представленная в таких доказательствах, по сути является цифровой, а не электронной. Этот вывод основан автором на анализе процессов кодирования и раскодирования информации. Также Н.В. Олиндер отмечает, что термин «цифровое доказательство» более точен, и предлагает авторское определение доказательств, содержащих цифровую информацию, подчеркивая необходимость представления таких доказательств в материальной форме[1].

Между тем Н.А. Зигура обращает внимание на то, что электронная среда основана на технических и программных средствах, функционирующих по строгим логическим правилам, в то время как аналоговая среда связана с человеческим восприятием и социальными нормами. Однако компьютерная информация не может быть непосредственно воспринята без использования специальных технических средств, что создаёт необходимость её преобразования в доступную для органов следствия и суда форму. При этом автор предлагает определение термина «компьютерной информации» как доказательства, подчёркивая, что это сведения в электронно-цифровой форме, созданные с использованием аппаратных и программных средств, которые после соблюдения процессуальных процедур могут быть использованы для установления обстоятельств дела. Н.А. Зигура также отмечает, что процесс формирования компьютерной информации как доказательства включает

[1] Олиндер Н.В. К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. Т. 3, № 3. С. 107–110.

многократное отображение данных, начиная с их создания программой и заканчивая фиксацией в процессуальных документах[1].

Собирание, проверка, оценка и использование доказательств в уголовном процессе играют ключевую роль, поскольку именно на их основе устанавливаются обстоятельства дела, принимаются процессуальные решения и выносятся итоговые судебные решения (п. 33, 53.2 ст. 5 УПК РФ). Между тем, доказывание представляет собой особый вид познавательной деятельности, регулируемой законом и осуществляемой уполномоченными субъектами, направленной на установление обстоятельств, входящих в предмет доказывания.

Согласно ст. 74 УПК РФ, доказательствами являются любые сведения, на основе которых суд, прокурор, следователь или дознаватель в установленном порядке определяют наличие или отсутствие значимых для уголовного дела обстоятельств[2]. Однако в российском законодательстве отсутствует четкое определение термина, этимологически сопряженного с электронной «начинкой» носителей, которые приобщаются к уголовному делу.

Главным образом, именно поэтому в современной уголовно-процессуальной доктрине такого рода электронные носители традиционно квалифицируются либо как вещественные доказательства, либо как иные документы, что обусловлено их двойственной природой. Критерий разграничения между этими категориями основывается на классическом доказательственном подходе: если доказательственное значение имеет материальный носитель информации с его физическими свойствами (например, поврежденный жесткий диск или флеш-накопитель со следами взлома), такие объекты следует относить к вещественным доказательствам. В случаях же, когда ценность представляет содержательная составляющая информации (текстовые файлы, базы данных, аудио- и видеозаписи), более обоснованным представляется их отнесение к иным документам.

---

[1] Зигура Н. А. Природа компьютерной информации как доказательства / Н. А. Зигура // Вестник Южно-Уральского государственного университета. Серия: Право. 2009. № 28(161). С. 50–52.

[2] Россинский С.Б. Доказательства по уголовному делу: требуется ли вносить коррективы в статью 74 УПК РФ? // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 161–171.

Обращение к доктринальным источникам, позволяет сделать вывод о том, что этой тематике было уделено достаточно внимания. Между тем, считаем наиболее приемлемым, под цифровой информацией в уголовном судопроизводстве понимать данные, представленные в электронной форме, зафиксированные на материальных носителях или передаваемые через информационно-телекоммуникационные сети, которые могут содержать сведения, имеющие значение для установления обстоятельств уголовного дела.

В отличие от традиционных вещественных доказательств, цифровая информация может существовать в идентичных копиях, что требует особых механизмов обеспечения ее достоверности и сохранности. Нематериальная природа доказательств, источником которых стала цифровая информация, представляет собой их фундаментальную характеристику. Поскольку передача данных осуществляется посредством бинарного кода и электромагнитных импульсов, такие доказательства лишены физического воплощения. Отсутствие материального носителя влечет за собой существенный риск несанкционированного изменения, удаления или переноса информации с сервера, расположенного в одной юрисдикции, на сервер другой страны. Данное обстоятельство обуславливает транснациональный характер цифровых доказательств, которые существуют в своеобразном метапространстве, выходящем за рамки традиционного сенсорного восприятия.

Список источников

1. Schetzen, M. (2005) Nonlinear system modeling based on the Wiener theory. *Proceedings of the IEEE,* vol. 69, no. 12, pp. C. 1557–1573.
2. Valentinov, V. (2017) Wiener and Luhmann on feedback: From complexity to sustainability. *Kybernetes*, vol. 46, no. 3, pp. 386–399.
3. Васюков В.Ф., Дамирчиев Э.И.О. Понятие и виды цифровой информации, используемой в доказывании по уголовным делам // Криминалистика: вчера, сегодня, завтра. 2025. № 2 (34). С. 38–50.
4. Духин, А.А. Теория информации : учебное пособие. Москва: Московский институт электроники и математики НИУ ВШЭ, 2005. 247 с.
5. Зигура Н. А. Природа компьютерной информации как доказательства // Вестник Южно-Уральского государственного университета. Серия: Право. 2009. № 28(161). С. 50–52.

6. Кремлев М.В. К вопросу о понятии информации, используемой в ходе расследования преступлений // Человек: преступление и наказание. 2014. № 4(87). С. 101–104.

7. Курилкина, В. Н. Философский и общенаучный анализ понятия информации / В. Н. Курилкина // Вестник Северо-Восточного федерального университета им. М.К. Аммосова. 2014. Т. 11, № 1. С. 73–77.

8. Макальский, Л. М. Информационная экология / Л.М. Макальский, А.К. Макаров, О.М. Цеханович; Под ред. Л.М. Макальского. Москва: ОнтоПринт, 2017. 48 с.

9. Маховиков А. Е. Информация в информационном обществе: проблема определения понятия // Наука XXI века: актуальные направления развития. 2020. № 1–2. С. 294–299.

10. Медведев Д.С. Категория истины в феномене "информация" / Д. С. Медведев // Журнал философских исследований. 2018. Т. 4, № 4. С. 41–45.

11. Мельситов В.В. Информация, коммуникация, трансляция / В. В. Мельситов, Н.Л. Сергиенко, З.К. Лакербай // Научные труды КубГТУ. 2017. № 6. С. 205–212.

12. Ожегов С.И. Словарь русского языка. М., 1978. С. 242.

13. Олиндер Н.В. К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. Т. 3, № 3. С. 107–110.

14. Подгорекци Ю. Смысловое значение понятия «информация» в коммуникативных процессах / Ю. Подгорекци, Н.А. Некрасова, С.И. Некрасов // Позиция. Философские проблемы науки, техники и образования. 2012. № 5. С. 198–209.

15. Россинский С.Б. Доказательства по уголовному делу: требуется ли вносить коррективы в статью 74 УПК РФ? // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 161–171.

16. Саттарова Н.И. Информация как коммуникация // Современное образование: содержание, технологии, качество. 2013. Т. 2. С. 7–8.

17. Соколов А.В. Философия информации: Учебное пособие. – 3-е изд. – Москва: Юрайт, 2020. 175 с.

18. Хромов Л.И. Теория информации и теория познания. СПб: Русское филос. общество, 2006. 200 с.

19. Цветков В.Я. Введение в теорию информации. М.: МАКС Пресс, 2007. 116 с.

Н.Б. Вахмянина
Московская академия Следственного комитета
имени А.Я. Сухарева

Проблемные аспекты допроса несовершеннолетних субъектов киберэкстремизма

Аннотация. В статье на основе анализа имеющихся классификаций типов несовершеннолетних субъектов преступления и свойств личности киберэкстремистов этой возрастной категории, автор делает вывод, что для прогнозирования развития следственной ситуации и планирования допроса последних представляет интерес степень радикализации направленности их личности. Также им предложена типология таких несовершеннолетних преступников и рассмотрены некоторые особенности их допроса.

Ключевые слова: киберэкстремизм, несовершеннолетние, допрос.

Исследованию тактики допроса несовершеннолетних субъектов преступлений посвящено достаточно много научных работ. Большинство ученых - криминалистов основывают разработку тактических приемов на свойствах личности, присущих этой категории. По мнению психологов, направленность является ведущим компонентом структуры личности.

Ряд криминологов и криминалистов обосновывают психологическую специфику, свойственную несовершеннолетним преступникам, криминогенной направленностью их личности. Соответственно этому критерию они выделяют типы: корыстный, корыстно-насильственный, насильственный[1].

Несомненно, следует согласиться и с учёными, которые в качестве классификационных критериев учитывают степень устойчивости антиобщественной направленности. Так, И.А. Макаренко выделяет следующие типы несовершеннолетних преступников: положительно-

[1]Антонян Ю.М. Криминология: учебник; Всероссийский научно-исследовательский институт МВД России. 2-е изд., перераб. и доп. М., 2012; Еникеев М.И. Общая, социальная и юридическая психология: Учебник для вузов. СПб., 2003 и др.

ситуативный, ситуативный, ситуативно-криминогенный, последовательно-криминогенный[1].

Несмотря на неоспоримую значимость научных трудов, описавших личностные свойства и качества несовершеннолетних каждой группы, в настоящее время их уже недостаточно. Современные реалии активного использования киберпространства для вовлечения несовершеннолетних в преступную деятельность и последующего совершения ими противоправных деяний требуют дополнения и переработки соответствующих научных рекомендаций. В.В. Бычков в рамках разработки научных основ борьбы с киберэкстремизмом уделял достаточно значительное внимание и аспектам проблематики расследования и профилактики данного вида преступлений, совершенных молодёжью[2]

Вовлечение молодых людей подросткового и юношеского возраста с использованием сети Интернет в деструктивные группы с целью дальнейшей обработки их сознания при помощи убеждающей коммуникации и навязывания им определенной системы ценностей является одним из распространенных способов изменения направленности их личности[3].

Как показывает практика, нередко такой обработке сознания поддаются не только дети с типами личности, характеризующимися криминогенной составляющей различного уровня развития, но и с социально-положительными личностно-мотивационными характеристиками личности. При этом некоторые из них самостоятельно начинают изучать радикальный контент экстремисткой направленности. Одни хотят удовлетворить

---

[1]Макаренко И.А. Личность несовершеннолетнего обвиняемого как объект криминалистического исследования. М., 2006. С. 85.

[2] Бычков В.В. Научные основы государственной программы борьбы с киберэкстремизмом. Москва., 2024.; Бычков В.В. Профилактика молодежного киберэкстремизма // Советская и российская криминалистика: традиции и перспективы : Материалы всероссийской научно-практической конференции с международным участием, Москва, 2 февраля 2023 г. М., 2023. С. 294–300 и др.

[3] Сироткина Т.Г. Вовлечение несовершеннолетних в совершение преступлений экстремистской направленности // Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики: V Всероссийская научно-практическая конференция молодых ученых (к 20-летию образования Московского университета МВД России имени В.Я. Кикотя): сборник научных трудов, Москва, 16 июня 2022 года / Сост. Р.Б. Осокин. М., 2022. С. 325.

любопытство, другие в поиске справедливости, помощи, третьи в поисках приключений.

Следует отметить, что мотивация для вступления подростка в экстремистскую группировку может быть противоречивой, не охватывать исключительно «идейный» уровень, а преследовать множественные цели, обусловленные материальными мотивами, стремлениями повысить социальный статус либо оказаться в поле внимания одноклассников, желанием пережить эмоции, связанные с риском, опасностью, повысить свою социальную защищенность за счет членства в группе[1].

Вместе с тем психологи отмечают, что при формирующейся экстремистской направленности личности проявляются такие черты, как «дистанцированность от других, отношение к другим с позиции превосходства, манипулятивность, нетерпимость к окружающим, стремление оправдать свои действия поведением других, возложить вину на окружающих, отказ от принятия на себя ответственности за происходящее, высокий уровень конфликтности, ненависть, гнев, обида, озлобленность и деструктивная мотивация по отношению к миру, его дегуманизация, негативизм и ориентация в поведении и деятельности на разрыв социальной коммуникации, односторонний отказ от диалога, разрыв социальных связей»[2].

Результат гибельного воздействия на сознание рассматриваемой возрастной категории предсказать не сложно - вовлечение в экстремистскую деятельность.

Для разработки тактических приемов допроса несовершеннолетних, совершивших преступления экстремисткой направленности, на наш взгляд, представляет наибольший интерес степень радикализации направленности их личности.

Подводя итог, можно выделить следующие типы несовершеннолетних, совершающих преступления экстремистского характера, в том числе с использованием сети Интернет:

1) с высокой степенью радикализации. Такие несовершеннолетние характеризуются устойчивостью сформированных радикальных

---

[1] Злоказов К.В. Психологические особенности вовлечения несовершеннолетних в экстремистские группировки // Психологический вестник Уральского федерального университета. Выпуск 10. Екатеринбург, 2013. С. 94.

[2] Беликова Е.В., Ефремов Е.Г. и др. Выраженность черт личности экстремисткой направленности у старшеклассников // Психолог. 2022. № 1. URL: https://nbpublish.com/library_read_article.php?id=36823

взглядов, враждебностью по отношению к окружающим, не поддерживающим их идеи, критической оценкой существующей социальной реальности, верой в исключительность догм поддерживаемой идеологии, установкой на немедленное изменение несовершенного порядка мироустройства, готовностью самопожертвованию, конфликтностью, регидностью, снижением способности к адекватной оценке ситуации.

2) со средней степенью – для них характерно также, как и первому типу слабая удовлетворенность социальных потребностей, стремление к уходу в трансцендентное, высокий уровень тревожности, но интерес к определенной деструктивной идеологии ещё не сформировался. Нередко они соглашаются оказать помощь своим друзьям из первой группы.

3) с низкой степенью – этот тип несовершеннолетних уже испытывает необходимость в поддержке, находится в поиске социальной группы, где могут её найти, но они не поддерживают радикальную идеологию, для них неприемлемы методы борьбы основанные на насилии. Либо их цели ограничены исключительно корыстным мотивом и ими руководит возможность быстро заработать деньги, либо эгоистичное желание обратить на себя внимание, самоутвердиться.

С учётом степени вовлеченности рассматриваемой возрастной группы в деструктивные идеологии представляется возможным спрогнозировать развитие следственной ситуации, направления противодействия и спланировать контрмеры.

Так, достаточно высока вероятность развития конфликтной или проблемно-конфликтной ситуации с несовершеннолетними из первой группы. Вместе с тем до их реабилитации с помощью психологов, а возможно и психиатров, из тактических приемов, на наш взгляд, могут быть доступны только умеренное проявление эмпатии по отношению к его личным проблемам и детализация данных им показаний, без их расширения в тех моментах, которые подросток умышленно игнорирует и проявляет негативные поведенческие реакции при упоминании о них.

Представляется, что попытки переубедить такого несовершеннолетнего без участия специалиста могут повлечь либо усугубление и без того непростой следственной ситуации, либо наступление более тяжелых последствий в виде проявления допрашиваемым аутоагрессии в форме суицидальных актов.

Допрос второй группы нередко осложняется по причине того, что такие субъекты преступлений экстремисткой направленности склонны объяснять свои поступки поведением других людей с перекладываем на них ответственности. При этом они зачастую не признают свою информированность об истинных причинах и целях выполнения ими общественно опасных действий, особенно если они действовали под руководством своих друзей, относящихся к первой группе.

В таких ситуациях в ходе допроса несовершеннолетнего – инициатора выполнения действий экстремистского характера, если он дает показания о событиях расследуемого преступления, необходимо детализировать их в части цели вовлечения других исполнителей. Кроме того, необходимо исследовать их переписку, изучаемый ими контент и его обсуждение в социальных сетях. Их одноклассники или знакомые их возраста также могут обладать информацией, подтверждающей осведомленность об истинных целях закупки, изготовления объектов, предметов для совершения преступлений рассматриваемого вида.

Может способствовать нейтрализации или минимизации противодействия несовершеннолетних второй группы демонстрация видеозаписи объяснений участников преступной группы, полученных сразу после их задержания. Участник противоправных событий из первой группы обычно раскрывает, хотя и кратко, основные обстоятельства и участников. При этом на фоне эмоционального возбуждения допускает множество оговорок, что позволяет применять такие видеозаписи для убеждения противодействующего субъекта в бессмысленности.

Следует отметить, что после демонстрации видеозаписи или её части следователю желательно изложить анализ просмотренного материала. Несовершеннолетний в силу высокого уровня тревожности, эмоционально напряженной обстановки и возрастной невнимательности к деталям может пропустить изобличающую его информацию.

Представляется, что к несовершеннолетним из третьей группы могут быть применены классические тактические приемы для допроса рассматриваемой возрастной группы субъектов преступлений.

Как уже неоднократно отмечалось в научной литературе, в ходе допроса любой из групп недопустимо проявление критического

отношения к взглядам несовершеннолетнего. Он может замкнуться, отказаться от дачи дальнейший показаний и демонстративно вызывающе себя вести в ходе проведения дальнейших следственных действий. Вероятность восстановления психологического контакта с несовершеннолетними первых двух групп представляется крайне низкой.

Список источников

1. Антонян Ю.М. Криминология: учебник. 2-е изд., перераб. и доп. М., 2012.
2. Беликова Е.В., Ефремов Е.Г., Ефремова Н.А., Кубарев В.С., Мильчарек Н.А., Мильчарек Т.П., Сенькова В.И., Френкель М.В., Цветкова О.А. Выраженность черт личности экстремисткой направленности у старшеклассников // Психолог. 2022. № 1. URL: https://nbpublish.com/library_read_article.php?id=36823
3. Бычков В.В. Научные основы государственной программы борьбы с киберэкстремизмом. М., 2024.
4. Бычков В.В. Профилактика молодежного киберэкстремизма // Советская и российская криминалистика: традиции и перспективы: Материалы всероссийской научно-практической конференции с международным участием, Москва, 2 февраля 2023 года. М., 2023. С. 294-300;
5. Еникеев М.И. Общая, социальная и юридическая психология: Учебник для вузов. СПб, 2003.
6. Злоказов, К.В. Психологические особенности вовлечения несовершеннолетних в экстремистские группировки // Психологический вестник Уральского федерального университета. Выпуск 10. Екатеринбург, 2013. С. 94–97.
7. Макаренко И.А. Личность несовершеннолетнего обвиняемого как объект криминалистического исследования. М., 2006.
8. Сироткина Т.Г. Вовлечение несовершеннолетних в совершение преступлений экстремистской направленности // Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики: V Всероссийская научно-практическая конференция молодых ученых (к 20-летию образования Московского университета МВД России имени В.Я. Кикотя): сборник научных трудов, Москва, 16 июня 2022 года / Сост. Р.Б. Осокин. М., 2022.

М.В. Галдин
Московская академия Следственного комитета
имени А.Я. Сухарева

О получении объяснений от несовершеннолетнего в ходе проверки сообщения о преступлении экстремистской направленности

Аннотация. Автор подчеркивает актуальность противодействия преступлениям экстремистской направленности и приводит данные судебной статистики. Характеризуя особенности первоначального этапа расследования преступления экстремистской направленности, выделяет процессуальные особенности производства следственных действий с несовершеннолетними, анализирует обоснованность их экстраполяции на получение объяснения в стадии возбуждения уголовного дела. Сделаны выводы о необходимости обеспечения участие законного представителя, адвоката и педагога (психолога) при проверке сообщения о преступлении.

Ключевые слова: досудебное производство по уголовным делам, стадия возбуждения уголовного дела, проверка сообщения о преступлении, преступления экстремистской направленности, несовершеннолетний, законный представитель несовершеннолетнего, адвокат, педагог, психолог.

Проблема противодействия экстремизму на постсоветском пространстве остается злободневной и особую актуальность ей придают события последних лет. С начала специальной военной операции по денацификации и демилитаризации Украины странами коллективного Запада была развязана полномасштабная информационная война против России. Ряд откровенных экстремистских проявлений расцениваются экспертами как военные преступления и акты терроризма[1].

По данным следственной практики, в качестве обвиняемых в совершении преступления экстремистской направленности чаще

[1] Бычков В.В. Следственно-оперативная характеристика преступлений экстремистской направленности // Вестник Московского университета МВД России. 2022. № 4. С. 52–57.

всего привлекаются лица мужского пола возрастом от 15 до 40 лет. В прошлом году за совершение таких преступлений был осужден 861 человек, из которых почти половина не достигли 39 лет, 22 из них – несовершеннолетние[1].

После выявления первичных признаков преступления экстремистской направленности следователю необходимо тщательно изучить поступившие материалы и оценить возможность формирования на их основе допустимых доказательств по уголовному делу. Не ограничиваясь этим, для установления оснований к возбуждению уголовного дела следователь должен провести проверку сообщения о преступлении в порядке, предусмотренном ст. 144 УПК РФ. В подавляющем большинстве случаев перед тем, как принять решение о возбуждении уголовного дела, следователь получает объяснение от лица, причастность которого проверяется к совершению преступления. Важность этого процессуального действия трудно переоценить: почти в 90% случаях такое лицо на первоначальном этапе расследования не только не отрицает свою причастность к совершению преступления, но и дает исчерпывающие пояснения о его обстоятельствах.

В стадии предварительного расследования закон предусматривает обеспечение несовершеннолетнего участием законного представителя, адвоката (в роли защитника или представителя), педагога или психолога (ст.ст. 45, 48, 51, 191, 425, 426 УПК РФ)[2]. Важно заметить, что обеспечивать участие законного представителя следует по уголовным делам о преступлениях, совершенных лицами, которым ко времени совершения преступления исполнилось четырнадцать, но не исполнилось восемнадцати лет (ст. 87 ч. 1 УК РФ, ст. 48 УПК РФ). Участие защитника при производстве процессуальных действий с лицом, совершившим преступление в

---

[1] Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции в 2024 г. // Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: https://cdep.ru (дата обращения 29.04.2025).

[2] Галдин М.В. Особенности проверки сообщения о совершенном несовершеннолетним преступлении экстремистской направленности // Актуальные проблемы противодействия экстремизму и терроризму на современном этапе: сб. науч. ст. IV Всероссийской научно-практической конференции с международным участием. Новосибирск: Новосибирский военный ордена Жукова институт имени генерала армии И.К.Яковлева войск национальной гвардии Российской Федерации, 2025. С. 114–115.

несовершеннолетнем возрасте, также признается в судебной практике обязательным независимо от того, достиг ли он к этому времени совершеннолетия (ст. 51 ч. 1 п. 2 УПК РФ). При решении вопроса о привлечении педагога (психолога), напротив, следует исходить из возраста на момент производства по уголовному делу. В следственной практике эти особенности часто экстраполируются на стадию возбуждения уголовного дела, что порождает вопросы об обязательности и обоснованности привлечения законного представителя, адвоката и педагога (психолога). Рассмотрим их на примере получения объяснения как наиболее востребованного действия.

Законный представитель обязан защищать права и интересы несовершеннолетнего в правоотношениях с любыми физическими и юридическими лицами (ст. 64 Семейного Кодекса РФ). В связи с этим он вправе участвовать на всех этапах процессуальной деятельности, начиная с момента приема сообщения о преступлении. Однако законный представитель вправе, а не обязан участвовать в доследственной проверке. Следователь должен известить его о месте и времени получения от несовершеннолетнего объяснения. Неявка законного представителя не препятствует производству данного проверочного мероприятия.

Право пользоваться услугами адвоката должно быть разъяснено любому участвующему в проверке сообщения о преступлении лицу. Если в отношении несовершеннолетнего проводится проверка сообщения о преступлении, то необязательность участия законного представителя при производстве процессуальных действий компенсируется обязательным присутствием адвоката при производстве любых процессуальных действий. Такое требование вытекает из анализа ст.ст. 51, 144 УПК РФ, руководящих разъяснений Пленума Верховного Суда РФ и ряда подзаконных нормативно-правовых актов[1].

---

[1] Постановление Пленума Верховного Суда РФ от 31.10.1995 N 8 (ред. от 03.03.2015) «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» (п. 17) // СПС КонсультантПлюс; Положение о возмещении процессуальных издержек, связанных с уголовным судопроизводством, издержек в связи с рассмотрением дела арбитражным судом, гражданского дела, административного дела, а также расходов в связи с выполнением требований Конституционного Суда Российской Федерации, утв. Постановлением Правительства РФ от 01.12.2012

Функция педагога (психолога) в уголовном судопроизводстве заключается в оказании следователю и суду помощи в установлении психологического контакта с несовершеннолетним, получении от него информации вербального свойства. Целесообразность его присутствия при получении от несовершеннолетнего объяснения определяется применением по аналогии иных норм процессуального закона (ст. ст. 425 ч. 3, 191 ч. 1 УПК РФ), а также криминалистическими рекомендациями.

В завершении важно отметить, что вне зависимости от того, участвовали при отобрании от несовершеннолетнего объяснения законный представитель, адвокат или педагог (психолог) или не участвовали, результаты этого процессуального действия не могут быть признаны доказательством в соответствии со ст.ст. 74, 75 и 144 УПК РФ. Требования о строго обязательном привлечении законного представителя и педагога (психолога) к получению объяснения от несовершеннолетнего следует признать не основанными на законе. Проблема здесь заключается в том, что результаты любых проверочных мероприятий не могут обладать всеми присущими доказательству свойствами, поскольку всегда имеют строго служебное значение, ограниченное принятием решения «внутри» и «для» стадии возбуждения уголовного дела. По этой причине следователь после возбуждения уголовного дела вынужден допрашивать ранее опрошенное лицо, то есть фактически делать двойную работу[1]. Такое положение не способствует экономии сил, средств и времени в досудебном производстве по уголовным делам и стимулирует исследователей на поиск пути совершенствования действующего законодательства.

N 1240 (п. 22(1) п.п. «в») // СПС КонсультантПлюс; Порядок назначения адвокатов в качестве защитников в уголовном судопроизводстве, утв. Решением Совета Федеральной палаты адвокатов от 15.03.2019, протокол № 4 (п. 2.4 п.п. 2) // Вестник Федеральной палаты адвокатов РФ, 2021. N 2.

[1] Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д.ю.н., д.т.н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. С. 179.

Список источников

1. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д.ю.н., д.т.н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. 572 с.
2. Бычков В.В. Следственно-оперативная характеристика преступлений экстремистской направленности // Вестник Московского университета МВД России. 2022. N 4. С. 52–57.
3. Галдин М.В. Особенности проверки сообщения о совершенном несовершеннолетним преступлении экстремистской направленности. Актуальные проблемы противодействия экстремизму и терроризму на современном этапе: сб. науч. ст. IV Всероссийской научно-практической конференции с международным участием // Новосибирск: Новосибирский военный ордена Жукова институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, 2025. С. 113–118.

Д.В. Галкин
Московская академия Следственного комитета
имени А.Я. Сухарева

О противодействии киберэкстремизму в рамках государственного контроля за использованием радиочастотного спектра

Аннотация. В статье рассматриваются возможности выявления, пресечения и расследования преступлений экстремистской направленности в рамках радиоконтроля во взаимодействии с радиочастотными центрами Роскомнадзора. Проанализированы имеющие правоохранительное значение функции и полномочия отдельных подразделений раиочастотных центров: мобильных групп радиоконтроля, центра правовой помощи гражданам в цифровой среде. Отмечены возможности взаимодействия радиочастотных центров со следственными и оперативными подразделениями правоохранительных органов.

Ключевые слова: расследование преступлений, киберэкстремизм, радиоразведка, радиоконтроль, взаимодействие следователя со специалистами, радиочастотные центры.

В круг научных интересов кандидата юридических наук, доцента Василия Васильевича Бычкова в последние годы его жизни входили вопросы противодействия преступлениям экстремистской направленности, в том числе совершаемые в сети Интернет. Разрабатывая теоретические основы борьбы с данным видом преступности, В.В. Бычков обосновывал научное значение термина «киберэкстремизм»[1].

Следуя в русле научных поисков В.В. Бычкова, отметим, что к киберэкстремизму относятся в том числе преступления, связанные с распространением в социальных сетях, мессенджерах и других сетевых ресурсах Интернета противоправного контента национального, политического, религиозного и иного содержания, несущего очевидно провокационный характер и способного возбуждать и разжигать деструктивную антисоциальную мотивацию (идеологию)[2].

Функции выявления и пресечения распространения такого контента, кроме правоохранительных и следственных органов, возложено на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и ее территориальные подразделения. Анализ осуществляемых полномочий и правоприменительной практики Роскомнадзора обращает внимание на потенциальную возможность распространения такого контента не только в указанных ресурсах сети Интернет, но и в радиоэфире средств массовой информации, осуществляющих радиовещание (радиостанций).

Указанное обстоятельство обуславливает актуальность взаимодействия следственных и оперативных подразделений правоохранительных органов с радиочастотными центрами, осуществляющими полномочия по государственному контролю за использованием радиочастотного спектра (радиоэфира). Несмотря на

---

[1] Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 26–31.

[2] Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. 2024. № 2. С. 54–58.

сокращение аудитории радиостанций в связи с развитием аудио- и видеоплатформ в Интернете, распространение экстремистской и иной противоправной информации в радиоэфире может представлять общественную опасность и нанести существенный вред охраняемым законом общественным интересам.

В криминалистической литературе обычно выделяется взаимодействие с радиочастотными центрами при выявлении и определении параметров работы базовых станций сотовой связи[1]. Вместе с тем, в практике работы радиочастотных центров имеется опыт выявления в радиоэфире правонарушений, связанных с распространением массовой информации. Так, в одном из районных центров на территории Дальневосточного федерального округа группой мобильного радиоконтроля проводились мероприятия по мониторингу радиоэфира, в ходе которого выявлено действие источника незаконного радиовещания. На частоте 90 МГц без разрешения на использование радиочастот и регистрации радиоэлектронных средств выходили в эфир программы на религиозную тематику. Аналоговый передатчик подпольной радиостанции был обнаружен в помещении магазина, принадлежащего местному индивидуальному предпринимателю. При содействии сотрудников правоохранительных органов и органов государственной безопасности незаконное вещание в радиоэфире было прекращено, материалы для привлечения виновных к ответственности направлены в территориальное подразделение Роскомнадзора[2].

В следственной практике имеют место и иные примеры участия специалистов радиочастотного центра в выявлении и раскрытии преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий. Так, в одном из регионов Сибири телекоммуникационная компания обратилась в

---

[1] Чирков П.С. О практике оценки радиоэлектронной обстановки на месте происшествия, получения и анализа информации об абонентах, абонентских устройствах и их соединениях // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: материалы Междунар. науч.-практ. конф., Москва, 17 окт. 2019 г. / под ред. А.М. Багмета. Москва, 2019. С. 636–639.

[2] Святое писание и грешное вещание: новости филиала ФГУП «ГРЧЦ» в Дальневосточном федеральном округе. URL: https://grfc.ru/grfc/filials/dfo/news/detail/index.php?ID=1648.

радиочастотный центр в связи с серьезными радиопомехами в работе одной из своих базовых станций. В ходе радиоразведки специалистами центра на бесхозном участке обнаружены несколько автомобилей, похищенных у законных владельцев и находящихся в розыске. С помощью радиопеленга рядом обнаружен являвшийся источником помех генератор радиошума – специальный источник широкополосного излучения, подавляющий работу автосигнализаций со встроенными SIM-картами. В ходе дальнейших оперативно-разыскных и следственных мероприятий личности автоугонщиков были установлены[1].

Таким образом, радиочастотные центры выполняют функции по радиоконтролю – узкоспециализированные, но имеющие важное значение в выявлении, пресечении и расследовании экстремистских и иных видов преступлений.

В настоящее время радиочастотные центры в Российской Федерации действуют в форме федерального государственного унитарного предприятия (ФГУП «ГРЧЦ») и его филиалов, подведомственного Роскомнадзору.

Уставными задачами ФГУП «Главный радиочастотный центр» являются осуществление организационных и технических мер по обеспечению надлежащего использования радиочастот и радиочастотных каналов, радиоэлектронных средств и высокочастотных устройств на территории России, содействие в выявлении нарушений в сфере использования радиочастотного спектра, оказания услуг связи, использования средств массовых коммуникаций и распространения информации.

ФГУП «Главный радиочастотный центр» имеет филиалы во всех федеральных округах России, а обособленные подразделения филиалов (управления) действуют в большинстве административных центров субъектов Российской Федерации. Радиочастотный центр – это предприятие (хозяйствующий субъект), обладающее технической базой для осуществления контроля за использованием радиочастот на обслуживаемой территории. Кроме стационарных комплексов, в филиалах центра функционируют группы мобильного радиоконтроля, оснащенные специальными техническими комплексами на базе малых автобусов (минивэнов). Для пеленга

[1] Новости филиала ФГУП «ГРЧЦ» в Сибирском федеральном округе. URL: https://grfc.ru/grfc/filials/sfo/news/detail/index.php?ID=42479.

радиочастот дополнительно используются носимые комплексы радиоконтроля и специальные средства измерений[1].

Технические возможности радиоконтроля, необходимые для получения криминалистически значимой информации, включают в себя:

- измерения и запись параметров излучений радиоэлектронных средств (РЭС), в том числе базовых станций операторов мобильной связи, без подключения к ним;
- определение местоположения РЭС (пеленг);
- определение принадлежности (собственника) РЭС, а при невозможности этого – определение координат места его установки и его описание для последующего установления собственника.

Кроме мониторинга радиоэфира, ФГУП «Главный радиочастотный центр» также участвует в выявлении противоправного контента в сетевых ресурсах Интернета. В структуре центра в 2021 году создан Центр правовой помощи гражданам в цифровой среде, его региональные офисы находятся в четырех городах: Москве, Санкт-Петербурге, Нижнем Новгороде и Новосибирске. Центр оказывает безвозмездную юридическую помощь гражданам по защите прав и законных интересов в связи с обработкой их персональных данных в сети Интернет, осуществляет правовое просвещение населения по вопросам безопасности использования информационно телекоммуникационных технологий, в случае выявления признаков преступлений в интересах граждан составляются заявления в правоохранительные органы[2].

Сотрудники разыскных и следственных подразделений совместно участвуют с представителями радиочастотных центров в рабочих группах и оперативных штабах по обеспечению проведения значимых общественных мероприятий[3]. Например, такое взаимодействие осуществлялось в ходе подготовки к Зимним

---

[1] Баранов В.П., Мельниченко А.Ю. Взаимодействие органов предварительного следствия и радиочастотной службы с целью проведения оценки радиоэлектронной обстановки // Вестник ГУК СК России. 2020. № 1(46). С. 20–23.

[2] Сайт Центра правовой помощи гражданам в цифровой среде ФГУП «Главный радиочастотный центр». URL: https://4people.grfc.ru/.

[3] Регламент взаимодействия территориальных органов Роскомнадзора с предприятиями радиочастотной службы. Утвержден приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 1186 от 23 октября 2013 г.

олимпийским играм 2014 года в Сочи, финалу чемпионата мира по футболу в 2018 г., летней универсиаде 2013 года в Казани и другим масштабным мероприятиям всероссийского и регионального уровня.

Список источников

1. Баранов В.П., Мельниченко А.Ю. Взаимодействие органов предварительного следствия и радиочастотной службы с целью проведения оценки радиоэлектронной обстановки // Вестник ГУК СК России. 2020. № 1(46). С. 20–23.
2. Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: Материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. Москва: Московская академия Следственного комитета Российской Федерации, 2023. С. 26–31.
3. Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. 2024. № 2. С. 54–58.
4. Чирков П.С. О практике оценки радиоэлектронной обстановки на месте происшествия, получения и анализа информации об абонентах, абонентских устройствах и их соединениях // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: материалы Междунар. науч.-практ. конф., Москва, 17 окт. 2019 г. / под ред. А.М. Багмета. Москва, 2019. С. 636–639.

Е.Н. Земскова
Московская академия Следственного комитета
имени А.Я. Сухарева

О некоторых проблемах применения уголовно-правовых норм о преступлениях террористического характера

Аннотация. В статье рассматриваются актуальные вопросы уголовно-правового противодействия организованным формам террористического характера. Проанализированы причины

недостаточно эффективной работы по их расследованию. Отмечены возможные пути решения имеющихся проблем.

Ключевые слова: организованная преступность, преступления террористической направленности, терроризм, террористическая организация, террористическое сообщество.

Терроризм является глобальной угрозой современного мира, его методы становятся все более жестокими и изощренными.

Разделяя озабоченность мирового сообщества беспрецедентным ростом актов терроризма, Россия в 2005 г. подписала и в 2006 г. ратифицировала Конвенцию Совета Европы о предупреждении терроризма [1], что стало отправной точкой для введения новых и трансформации действующих уголовно-правовых норм в целях их адаптации к положениям Конвенции и существующим реалиям.

Так, 2013 г. в связи с обострением политической ситуации на Ближнем Востоке и вовлечением российских граждан в деятельность незаконных вооруженных формирований, в том числе на территориях иностранных государств, Федеральным законом от 02.11.2013 № 302-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[2] УК РФ дополнен нормами, устанавливающими ответственность за организованные формы террористической деятельности, – ст. ст. 205.4 (организация террористического сообщества и участие в нем), 205.5 (организация деятельности террористической организации и участие в деятельности такой организации).

В научных кругах до настоящего времени не прекращаются дискуссии о целесообразности введения уголовной ответственности за два, по сути схожих, деяния[3].

---

[1] Конвенция Совета Европы о предупреждении терроризма ETS № 196 (Варшава, 16 мая 2005 г.) // СЗ РФ. 2009. № 20. Ст. 2393.

[2] СЗ РФ. 04.11.2013. № 44. Ст. 5641.

[3] См., например: Сипки М.О. О практике применения статей 205.4 и 205.5 УК РФ // Актуальные проблемы российского права. 2018. №1 (86). URL: https://cyberleninka.ru/article/n/o-praktike-primeneniya-statey-205-4-i-205-5-uk-rf (дата обращения: 12.04.2025); Кондратенко З.К. К вопросу об определении уголовно-правовых понятий «террористическое сообщество» и «поддержка терроризма» // Наука и современность. 2015. № 4 (6). С. 98-107.

Согласно постановлению Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности»[1], террористическое сообщество представляет собой устойчивую группу лиц, заранее объединившихся в целях осуществления террористической деятельности либо для подготовки или совершения одного либо нескольких преступлений террористического характера, либо иных преступлений в целях пропаганды, оправдания и поддержки терроризма.

Понятие же «террористическая организация» не раскрывается ни в вышеназванном постановлении, ни в Федеральном законе от 06.03.2006 № 35-ФЗ «О противодействии терроризму»[2], несмотря на то, что террористическая организация является ключевым элементом терроризма, обладает высшим уровнем структурированности и организованности, ей «свойственно продолжение деятельности, несмотря на запрет данной организации, что свидетельствует о весьма высоком ресурсе и наличии влиятельных источников, позволяющих продолжать существование организации»[3].

В соответствии с указанным законом организация признается террористической и подлежит ликвидации (ее деятельность – запрещению) по решению суда на основании заявления Генерального прокурора Российской Федерации или подчиненного ему прокурора в случае, если от имени или в интересах организации осуществляются организация, подготовка и совершение террористических преступлений, а также если указанные действия осуществляет лицо, которое контролирует реализацию организацией ее прав и обязанностей. Террористической организацией, деятельность которой подлежит запрещению, также признается террористическое сообщество при наличии вступившего в законную силу обвинительного приговора в отношении лица за создание террористического сообщества, руководство им или участие в нем.

Террористическое сообщество может существовать как в форме организованной группы, так и в форме преступного сообщества, при этом для его функционирования важна цель – подготовка или

---

[1] БВС РФ. № 4. Апрель, 2012.

[2] СЗ РФ. 13.03.2006. № 11. Ст. 1146

[3] Тихонин И.А. Разграничение организации террористического сообщества и деятельности террористической организации для целей уголовного закона // Вопросы российской юстиции. Вып. № 20. 2022. С. 521.

совершение преступлений, прямо указанных в ст. 205.4 УК РФ. Такое сообщество характеризуется устойчивостью, наличием двух или более физических вменяемых лиц, в том числе организатора, достигших установленного законом возраста уголовной ответственности, предварительного сговора между ними на совершение террористических преступлений.

Для признания группы лиц по предварительному сговору (организованной группы) террористическим сообществом не требуется предварительного судебного решения о ликвидации организации в связи с осуществлением террористической деятельности.

Исходя из приведенных законодателем формулировок, отличие террористической организации от террористического сообщества состоит в наличии вступивших в законную силу решения суда о признании организации террористической или обвинительного приговора в отношении конкретного лица, создавшего либо участвовавшего в деятельности террористического сообщества.

Анализ статистических данных ФГКУ «ГИАЦ МВД России»[1] за 2022-2024 гг. свидетельствует о незначительном числе находившихся в производстве преступлений об организации террористического сообщества и организации деятельности террористической организации (ч. 1 ст. 205.4 и ч. 1 ст. 205.5 УК РФ), соответственно, и отсутствии устойчивой положительной динамики результатов их расследования.

На наш взгляд, это связано не со спадом террористической активности, а скорее всего – с повышением уровня конспирированности террористических формирований, ростом количества «спящих» террористических ячеек, что затрудняет выявление и пресечение их незаконной деятельности.

Так, в 2022, 2023, 2024 гг. в производстве следователей находились уголовные дела о 58, 41, 43 преступлениях, предусмотренных ч. 1 ст. 205.4 УК РФ, соответственно. В суды направлены уголовные дела о 5, 8, 10, прекращены – о 2 (п. 4 ч. 1 ст. 24 УПК РФ), 0, 0 преступлениях.

По ч. 1 ст. 205.5 УК РФ в указанные годы в производстве находились уголовные дела о 27, 15, 21 преступлениях,

[1] По данным формы статистической отчетности «Сведения о преступлениях террористической направленности», сформированной за январь-декабрь 2022, 2023, 2024 гг. // Информационный ресурс МВД России.

соответственно. В суды направлены уголовные дела о 10, 5, 9, прекращены – о 2 (п. 4 ч. 1 ст. 24 УПК РФ), 0, 0 преступлениях.

Количество расследованных преступлений, сопряженных с участием в террористическом сообществе (ч. 2 ст. 205.4 УК РФ), ежегодно приблизительно в 10 и более раз меньше числа преступлений, сопряженных с участием в террористической организации (ч. 2 ст. 205.5 УК РФ).

Так, в 2022-2024 гг. в производстве следователей находились уголовные дела о 24, 42, 75 преступлениях, предусмотренных ч. 2 ст. 205.4 УК РФ, соответственно. В суды направлены уголовные дела о 2, 12, 25, прекращены – 0, 0, 1 (по п. 1 ч. 1 ст. 24 УПК РФ) преступлениях.

По ч. 2 ст. 205.5 УК РФ в производстве находились уголовные дела о 513, 484, 617 преступлениях, соответственно. В суды направлены уголовные дела о 73, 80, 172, прекращены – о 14, 6, 14 (ст. 28 УПК РФ – 6, 3, 7; п. 4 ч. 1 ст. 24 УПК РФ – 8, 3, 7) преступлениях.

Полагаем, что сложившаяся ситуация обусловлена не только фактическим состоянием преступности, сопряженной с организованными формами террористической деятельности, но и существующими проблемами правоприменения.

Законодательные новеллы, касающиеся ответственности за схожие формы организованной террористической деятельности, при этом имеющие существенные отличия по признакам объективной и субъективной сторон как между собой, так и от преступного сообщества (преступной организации) – ст. 210 УК РФ, – создает определенные сложности в формировании доказательной базы при расследовании уголовных дел о таких преступлениях.

Доказывание фактов сговора между участниками террористического сообщества на совершение террористических преступлений, тесных взаимосвязей между ними, согласованности их действий, наличия структурных подразделений, постоянства форм и методов преступной деятельности, длительности ее осуществления и количества совершенных преступлений требуют от следователя, помимо творческого подхода к решению следственных задач, значительных организационных, материальных и временных затрат. Несколько более простым представляется расследование организации деятельности террористической организации и участия в ней, поскольку в данном случае достаточно установить факты наличия вступившего в законную силу решения суда о признании

организации террористической, а также проведения бесед, собраний, организации шествий в целях пропаганды деятельности запрещенной организации либо непосредственного участия в проводимых организационных мероприятиях.

Подводя итог, следует отметить, что для более успешного противодействия организованной террористической деятельности с учетом сложившейся следственно-судебной практики необходим комплексный подход, включающий внесение изменений в действующие нормы УК РФ, подготовку Верховным Судом Российской Федерации разъяснений, касающихся конкретизации понятий «террористическое сообщество» и «террористическая организация», их признаков, отличия от преступного сообщества, с целью обеспечения единообразного применения соответствующих уголовно-правовых норм, а также разработку методических рекомендаций по раскрытию, расследованию и профилактике рассматриваемых преступлений.

Список источников

1. Конвенция Совета Европы о предупреждении терроризма ETS № 196 (Варшава, 16 мая 2005 г.) // СЗ РФ. 2009. № 20. Ст. 2393.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.
3. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // СЗ РФ. 13.03.2006. № 11. Ст. 1146.
4. Постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // БВС РФ. № 4. Апрель, 2012.
5. Кондратенко З.К. К вопросу об определении уголовно-правовых понятий «террористическое сообщество» и «поддержка терроризма» // Наука и современность. 2015. № 4 (6). С. 98–107.
6. Сипки М.О. О практике применения статей 205.4 и 205.5 УК РФ // Актуальные проблемы российского права. 2018. №1 (86). URL: https://cyberleninka.ru/article/n/o-praktike-primeneniya-statey-205-4-i-205-5-uk-rf (дата обращения: 12.04.2025).
7. Тихонин И.А. Разграничение организации террористического сообщества и деятельности террористической организации для целей

уголовного закона // Вопросы российской юстиции. Вып. № 20. 2022. С. 516-524.

8. Статистическая отчетность «Сведения о преступлениях террористической направленности» ФКУ «ГИАЦ МВД России», сформированной за январь-декабрь 2022, 2023, 2024 гг. // Информационный ресурс МВД России.

С.В. Зуев
Южно-Уральский государственный университет
(национального исследовательского университета)

Совершенствование оперативно-разыскных средств борьбы с экстремизмом в сети Интернет

Аннотация. Данная статья посвящена проблемам борьбы с экстремизмом в сети Интернет. Предлагаются меры по совершенствованию оперативно-разыскного законодательства. В частности, перечень оперативно-разыскных мероприятий следует дополнить таким, как «Мониторинг сети Интернет». Требуется также четкое разграничение таких оперативно-разыскных мероприятий, как «Получение компьютерной информации» и «Снятие информации с технических каналов связи». Указывается, что обязательное условие на получение судебного решения для проведения оперативно-разыскного мероприятия «Получение компьютерной информации» неоправданно усложняет оперативную работу.

Ключевые слова: экстремизм, борьба с преступностью, оперативно-разыскная деятельность, оперативно-разыскные мероприятия, оперативно-разыскной закон.

Противодействие экстремизму как негативному явлению должно осуществляться надлежащими правовыми средствами, в том числе в сфере оперативно-разыскной деятельности. Интернет в настоящее время представляет собой не только информационно-коммуникационную среду, но и место борьбы с такими угрозами обществу и государству, как экстремизм и терроризм.

Ю.А. Лапунова отмечает, что противодействие экстремизму в сети Интернет требует качественно новых подходов[1]. В развитии этого хочется обратить внимание на перечень оперативно-разыскных мероприятий, предусмотренных ст. 6 Федерального закона «Об оперативно-разыскной деятельности». С учетом современных реалий, в данный перечень следовало бы включить такое оперативно-разыскное мероприятие, как «Мониторинг сети Интернет», что позволило бы сотрудникам оперативных подразделений на законных основаниях изучать социальные сети и сайты в поисках информации о противозаконной деятельности.

Принимая во внимание, что на сегодня суды рассматривают результаты оперативно-разыскных мероприятий наравне с доказательствами, полученными следователем или дознавателем, следовало бы распространять на результаты оперативно-разыскной деятельности требования допустимости доказательств. Тому подтверждение и положение ст. 89 УПК РФ, по смыслу которой результаты данной деятельности должны отвечать требованиям, предъявляемым к доказательствам.

Справедливо считать, что доказывание по уголовным делам может осуществляться только в рамках тех правовых средств, которые предусмотрены действующим законодательством. Результаты любых действий и мероприятий, не предусмотренных законом, не могут ложиться в основу приговора, вынесенного судом.

Представляется также, что относительно такого оперативно-разыскного мероприятия, как «Получение компьютерной информации» необходимо исключить обязательное требование – получение судебного решения. Причин тому несколько. Во-первых, оперативно значимая информация не всегда может затрагивать чьи-то конституционные права, ограничение которых возможно только по судебному решению. Во-вторых, обращение органов, осуществляющих оперативно-разыскную деятельность, в суд, в отсутствии межведомственного электронного взаимодействия, требует дополнительного времени и снижает оперативность. В-третьих, оперативным сотрудникам в целом следовало бы оказывать больше доверия, поощрять их инициативность, самостоятельность в решении оперативных задач.

---

[1] Лапунова Ю.А. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. 2017. № 3 (43). С. 102.

Кроме того, существует проблема разграничения таких оперативно-разыскных мероприятий, как «Получение компьютерной информации» и «Снятие информации с технических каналов связи». А.Л. Осипенко верно указывает на то, что первое такое оперативно-разыскное мероприятие «отражает не способ получения оперативно-разыскной информации, а форму, в которой эта информация представлена»[1].

Согласно ст. 272 УК РФ компьютерная информация – это «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Под электрическими сигналами можно понимать частоты в световом спектре, которые могут быть зафиксированы и воспроизведены компьютерной техникой, то есть персональными компьютерами, ноутбуками, планшетами, смартфонами. Такая информация может находиться в свободном доступе, что более характерно для проведения оперативно-разыскного мероприятия «Получение компьютерной информации». Проведение же оперативно-разыскного мероприятия «Снятие информации с технических каналов связи» направлено на сканирование технического канала, радиоперехват, копирование и другие действия фиксации информации на магнитных, электронных и бумажных носителях. К техническим относят каналы электросвязи, используемые для передачи и приема сигналов, знаков, текста, изображений, звуков при помощи технических средств по проводной, радио- и другим электромагнитным системам. Для проведения этого могут быть привлечены сотрудники предприятий, организаций, чьи технические каналы и средства связи задействованы для снятия информации. Мероприятие может проводиться и специализированными оперативными подразделениями ОВД и ФСБ с использованием собственных специальных технологий, технических и аппаратных средств[2].

Особое значение приобретает метод негласного применения специального программного обеспечения для получения закодированной информации, хранящейся на компьютере или смартфоне. Для этого задействуют специалистов бюро специальных

---

[1] Осипенко А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 84.

[2] Зуев С.В. Основы оперативно-розыскной деятельности: учебное пособие для вузов. М., 2020. С. 121.

технических мероприятий или провайдеров. Использование вирусных программ является распространенной практикой за рубежом. Данные действия предусмотрены, к примеру, в УПК Германии и других стран. Представляется, что и в Российской Федерации в уголовно-процессуальном кодексе следовало бы закрепить ряд негласных следственных действий. Данный вопрос уже неоднократно рассматривался в литературе[1].

Многие знают о применении в решении оперативных и разведывательных задач такой метапоисковой системы, как OSINT[2]. Кроме этого, можно использовать и другие высокотехнологические средства получения информации для противодействия экстремизму и терроризму. К этому относится, к примеру, HUMINT; SIGINT, COMINT, ELINT; IMINT; GEOINT; FININT; TECHINT; CYBINT (DNINT)[3]. В перспективе следует ожидать применение технологий искусственного интеллекта для поиска киберэкстремистов в сети Интернет, посредством мобильной телефонии, камер систем видеонаблюдения, спутниковой навигации, в том числе изменивших внешность с помощью пластических операций[4], что, возможно, потребует внесения соответствующих дополнений в оперативно-разыскное законодательство.

В информационной войне с преступностью требуются современные средства и методы противодействия, включая работу всех правоохранительных органов, прокуратуры и суда. Только так можно добиться информационного превосходства и реализации принципа неотвратимости наказания за совершенные действия экстремистского характера. Доказательствами экстремизма могут выступать сведения, полученные при обнаружении и фиксации электронной информации в сети Интернет. При этом надо учитывать, что установление лица, распространяющего информацию экстремистского характера, может

---

[1] См. подробнее об этом: Зуев С.В. Негласные следственные действия в уголовном судопроизводстве // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2016. № 16-1. С. 152-154.

[2] OSINT – совокупности знаний и навыков, позволяющих идентифицировать человека по используемым им телекоммуникационным каналам.

[3] URL: https://osintteam.blog/intelligence-gathering-disciplines-osint-imint-geoint-etc-7d9bbdd7f43f

[4] Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. 2022. № 1. С. 63.

быть осложнено ввиду анонимности, закрытости аккаунта, попытки скрыть свои данные и доказательства при возникновении подозрения в разоблачении.

Подводя итог, следует заметить, что эффективно бороться с экстремизмом и терроризмом можно только общими усилиями правоохранительных органов, применяя, в том числе негласные методы оперативной работы, а также современные технологии, включая системы искусственного интеллекта. Борьба с преступностью должна вестись надлежащими, то есть соответствующими действительности и криминальным угрозам, правовыми средствами.

Список источников

1. Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. 2022. № 1. С. 60–65.

2. Зуев С.В. Негласные следственные действия в уголовном судопроизводстве // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2016. № 16-1. С. 152–154.

3. Зуев С.В. Основы оперативно-разыскной деятельности: учебное пособие для вузов. М.: Юрайт. 2020. 191 с.

4. Лапунова Ю.А. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. 2017. № 3 (43). С. 100–104.

5. Осипенко А.Л. Новое оперативно-разыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 83–89.

И.Н. Кожевников
Адвокатское бюро «Ри-консалтинг»,
г. Москва, соискатель

К вопросу о криминологических показателях преступлений в области газовой промышленности

Аннотация. Автор исследует состояние преступности в области газовой промышленности, вследствие чего, с одной стороны, приходит к выводу, что по сегодняшний день в Российской Федерации не ведется открытой статистической отчетности в данной области, с другой – предлагает ее ввести и использовать соответствующие критерии при ее формировании.

Ключевые слова: газовая промышленность, криминологические показатели, количественные признаки, качественные признаки, динамика преступности.

Криминологические показатели преступности представляют собой числовые данные, которые демонстрируют уровень и динамику преступности как в отдельном государстве (национальные показатели), так и в целом в международном сообществе (международные показатели). Благодаря анализу таких сведений представляется возможным корректировать уголовную политику, а также прогнозировать тенденции увеличения или спада той или иной преступности. Криминологами выработан термин «обобщающие показатели преступности», под которым предлагается понимать относительные или средние показатели преступности, характеризующиеся всю или определенную часть совокупности статистических данных о преступности, личности преступников, причинах и условиях преступности, результатах профилактической деятельности[1].

В контексте избранной темы исследования следует отметить, что субъекты (Главный информационно-аналитический центр МВД России, Генеральная прокуратура Российской Федерации и Судебным департамент при Верховном Суде Российской Федерации)

[1] Криминология: Учебное пособие / под общ. ред. В.Е. Эминова. М.: Изд. группа ИНФРА-М; НОРМА, 1997. С. 71.

формирующие статистические данные о преступности, не выделяют отдельно преступления, совершенные в области газовой промышленности, что делает, с одной стороны, затруднительным их анализ, но, с другой стороны, это не означает, что такие данные не представляется возможным вычленить из общего массива и обобщить. Отчасти этот фактор сыграл особую роль при выборе критериев классификации преступлений, совершенных в области газовой промышленности. Именно обращение к составам преступлений представляется возможным выделить рассматриваемые нами преступлений и дать характеристику криминологическим показателям. Если обратиться к статистическим сведениям, которые обобщены Судебным департаментом при Верховном Суде Российской Федерации, можно лишь выделить один состав преступления, который с учетом нормативного подхода относится к области газовой промышленности. Речь идет о ст. 215.3 УК РФ диспозиция указывает на действия, связанные с самовольным подключением к нефтепроводам, нефтепродуктопроводам, газопроводам. Так, за 2024 год всего осуждено по ст. 215.3 УК РФ – 1 050 (ч.1); 0 (ч. 2); 1 (ч. 3); и 9 (ч. 4)[1].

Иных специальных данных, которые могут быть применимы в криминологических целях упомянутый федеральный государственный орган не приводит. В этой связи нет смысла приводить общие статистические сведения по отдельным преступлениям, которые могут быть совершены в области газовой промышленности. Привести абсолютные показатели количества преступлений в области газовой промышленности не представляется возможным в виду отсутствия соответствующего раздела в статистической отчетности, если даже предпринять попытку оперировать только конкретными составами преступлений. Вместе с тем не стоит исключать, что даже представление данных о количестве зарегистрированных преступлений в области газовой промышленности и выявленных лиц, причастных к их совершению, это не позволит в полной мере уяснить современные криминологические реалии, поскольку многие из таких преступлений будут иметь латентный характер. Именно обобщение

[1] Отчет о числе привлеченных к уголовной ответственности и видах уголовного наказания // Судебный департамент при Верховном Суде Российской Федерации. URL: https://cdep.ru/index.php?id=79&item=8946 (дата обращения: 01.06.2025).

зарегистрированных преступлений, принимая одновременно во внимание и латентные общественно опасные деяния в данной сфере, позволят с высокой степенью достоверности говорить о состоянии *реальной* преступности в газовой промышленности. Зачастую эксперты подмечают, что латентная преступность превышает зарегистрированную в десять раз[1]. С данным предположением можно согласиться, если тем более сделать акцент на преступлениях коррупционной направленности в области газовой промышленности.

Безусловно, что «реальная картина дел» связана с динамикой, темпами роста или снижения преступности, в особенности, если говорить об отдельных преступлениях в области газовой промышленности. Допустим, в одном регионе наблюдается прирост краж, совершенных из газопровода (п. «б» ч. 3 ст. 158 УК РФ), а другом субъекте Российской Федерации, наоборот, усматривается снижение (спад) таких общественно опасных деяний за аналогичный период времени. Только суммировав эти данные можно говорить о конкретном состоянии преступности в области газовой промышленности.

Немаловажное значение для оценки состояния преступности в области газовой промышленности играют данные об удельном весе преступлений по степени тяжести (небольшой, средней тяжести, тяжкие и особо тяжкие), по формам и видам вины (умышленные и неосторожные), по видам мотивации (корыстные или легкомысленные), по субъектам преступления (мужчины, женщины, несовершеннолетние, безработные или должностные лица), по характеру и размерам причиненного вреда (ущерба) и так далее. Во всех случаях стоит учитывать так называемую «*географию*» преступности, то есть распространение ее в отдельных административно-территориальных образованиях.

Также особую роль играет феномен динамики преступности, который отражает изменение преступности во временном промежутке. Общепринято принимать один год, но все зависит от цели и характера исследования той или иной преступности. В последнее время усматривается также тенденция так называемой «цифровой» преступности, а точнее увеличивается число преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной

[1] См.: Муслов Б.В. Латентная преступность: некоторые вопросы теории и практики противодействия: дис. … канд. юрид. наук. СПб., 2006.

информации. Так, в январе-декабре 2024 года зарегистрировано 765,4 тыс. указанных преступлений, что на 13,1 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе-декабре 2023 года до 40,0%[1]. Учитывая, что под преступлениями, совершенными с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, понимаются любое общественно опасное деяние, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети[2]. Среди самых распространенных стоит выделить использование фальшивых квитанций для оплаты услуг поставки газа, которые вкладывают в почтовые ящики в жилище потерпевших или направляются в электронной форме по их электронной почте. Не следует также исключать и ситуации, когда в ходе «физической» кражи, совершенной из газопровода (п. «б» ч. 3 ст. 158 УК РФ), или действий, связанных с самовольным подключением к газопроводам, злоумышленники использовали различные аппаратные или программно-аппаратные комплексы, облегчающие совершения таких преступлений. Как представляется, такие особенности вычленения преступлений в области газовой промышленности из объема общественно-опасных преступлений, совершенных с использованием электронных или информационно-телекоммуникационных сетей, стоит учитывать при установлении количественных показателей.

Не следует также исключать из объема общественно опасных деяний в области газовой промышленности, которые должны учитываться в рамках подсчета криминологических показателей и

---

[1] См.: Состояние преступности в России за январь-декабрь 2024 года, подготовленный Главным информационно-аналитическим центром Министерства внутренних дел Российской Федерации // Министерство внутренних дел Российской Федерации [Электронный ресурс]. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 01.07.2025).

[2] Пункт 20 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет” // Бюллетень Верховного Суда Российской Федерации. 2023. № 3.

преступления в сфере компьютерной информации (Глава 28 УК РФ). Докажем это следующим примером. *Так, К. совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекшее копирование компьютерной информации из корыстной заинтересованности, при следующих обстоятельствах. К., умышленно, действуя из корыстной заинтересованности с целью незаконного получения материальной выгоды, находясь в помещении ООО «Газпром Межрегионгаз Махачкала» осуществил неправомерный доступ к охраняемой законом компьютерной информации, скопировал базу данных ООО «Газпром Межрегионгаз Махачкала», в последующем позволяющее ему беспрепятственно и несанкционированно принимать платежи за потребляемых ими природный газ от индивидуальных предпринимателей*[1].

По этому же принципу стоит учитывать также и преступления, связанные с неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ). В соответствии со ст. 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2] под ней понимают объекты критической информационной структуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Как представляется к таковой следует отнести и газоснабжающую организацию[3].

В этой связи при проведении криминологических показателей преступности в области газовой промышленности играют ее *качественные признаки*, которые в общем раскрывают *структуру* и *характер* деяний. Под структурой преступности в криминологии понимают как: 1) совокупность всех преступлений, совершенных в той или иной стране, регионе за конкретный период, либо исторический момент, распределенная по видам, где последние рассматриваются рядом группировочных признаков, а наиболее важные из них – социально-демографические, уголовно-правовые и

[1] Приговор Советского районного суда города Махачкалы от 28 сентября 2020 года № 1-769/2020 // Справочно-правовая система КонсультантПлюс.

[2] Собрание законодательства Российской Федерации. 2017. № 31 (Часть I). Ст. 4736.

[3] См. приговор Беловского городского суда Кемеровской области от 28 мая 2024 года по делу № 1-415/2024 года // Справочно-правовая система КонсультантПлюс.

криминологические[1]; 2) основной качественный показатель преступности, раскрывающий внутреннее содержание данного социально-негативного явления, соотношение различных форм или отдельных видов преступности в общем числе зарегистрированных преступлений, где структурные элементы, в зависимости от целей анализа и иных обстоятельств, могут выделяться по самым разнообразным группировочным признакам[2].

Характер же преступности проявляется в ином, поскольку определяется числом наиболее опасных (тяжких) преступлений в структуре преступности, а также характеристикой личности злоумышленников, но которая выявляется через ее структуру[3]. В контексте избранной темы исследования можно предположить, что характер преступлений в области газовой промышленности будет определяться исходя из следующей классификации таких преступлений: 1) кража, совершенная из нефтепровода, нефтепродуктопровода, газопровода (п. «б» ч. 3 ст. 158 УК РФ); 2) действия, связанные с самовольным подключением к нефтепроводам, нефтепродуктопроводам и газопроводам (ст. 215.3 УК РФ); 3) неосторожные преступления, связанные с нарушением требований правил безопасности (ст. 109 УК РФ, ст. 217 УК РФ); 4) хищения (ст. 158, 159, 160 УК РФ); 5) причинение ущерба путем обмана или злоупотреблением доверием (ст. 165 УК РФ); 6) незаконное предпринимательство (ст. 171 УК РФ); е) коррупционные преступления (ст. 204 УК РФ, 290-291 УК РФ); 7) приведение в негодность объектов жизнеобеспечения; 8) производство, хранение, перевозка либо сбыт товаров и продукции, выполнение работ или оказание услуг, не отвечающих требованиям безопасности (ст. 238 УК РФ). Также предлагается выделять такие преступления в зависимости от различных этапов их совершения, а именно: 1) в ходе добычи газа; 2) при транспортировке газа; 3) при переработке газа; 4) при распределении газа.

Что же касается характера преступлений в области газовой промышленности, прежде всего следует учитывать какое из

---

[1] Каиржанов Е. Криминология (общая часть). Алматы: Республиканский издательский кабинет, 1995. С. 6.

[2] Алексеев А.И. Криминология. Курс лекций. М.: Изд-во «Щит-М», 1998. С. 31–32.

[3] Криминология. Учебное пособие / Под общ. ред. В.Е. Эминова. М.: Изд. группа ИНФРА-М; НОРМА, 1997. С. 95.

описанных выше общественно опасных деяний представляет большую общественную опасность, что, кстати не всегда просто учесть, а также тяжесть, которая определяется с учетом ст. 15 УК РФ и рецидивности. К примеру, если сравнивать п. «в» ч. 3 ст. 158 УК РФ и ч. 5 ст. 215.3 УК РФ именно последнее будет считаться более тяжким, поскольку предусматривает наказание в виде лишения свободы на срок до восьми лет при наступлении по неосторожности смерти человека или иные тяжкие последствия. К глубокому сожалению, открытых статистических данных не имеется для того, чтобы провести соответствующий криминологический анализ. Безусловно, стоит учитывать при определении структуры преступности в области газовой промышленности распределение по мотивам, доли ситуативной, профессиональной, групповой и организованной преступности; удельный вес раскрытых и нераскрытых, а также доли личностей (мужчины, женщины и несовершеннолетних и т.д.). Между тем не следует сбрасывать со счетов тот фактор, что собственно структура преступности составляет ее характер, степень опасности, закономерные связи с различными явлениями объективной реальности, вследствие чего преступность в области газовой промышленности детерминируется, с одной стороны, экономическими процессами, что в особенности проявляется при хищении газа и самовольном подключении к газопроводам, а, с другой стороны, социально-психологическими процессами, которые наиболее наглядно прослеживаются в ходе неосторожных преступлений против личности (нарушение правил безопасности при использовании газового оборудования). С точки зрения структуры «газовой преступности» можно выделить следующее социальное содержание мотивации, оставляя за скобками, нормативно-правовой критерий (уголовно-правовой): 1) корыстные и 2) легкомысленно – безответственные[1]. Благодаря характеристике общественно опасных деяний с учетом их многовариативных компонентов позволяет проанализировать криминологическую обстановку более «реально» как в Российской Федерации, так и в отдельных ее регионах.

Таким образом, резюмирую все изложенное выше, можно сформулировать ряд выводов.

[1] См.: Кудрявцев В.Н., Лунеев В.В. О криминологической классификации преступлений // Государство и право. 2005. № 6. С. 54–66.

1. В силу отсутствия открытых статистических данных о состоянии преступности в области газовой промышленности дать точную характеристику таких криминологических показателей не представляется возможным. Это обусловлено тем, что субъекты, ведущие «криминальную» статистику, не выделяют такую специфическую и отдельную группу преступлений. Между тем некоторые общественно опасные деяния все же могут быть объектом криминологического анализ и прогнозирования (например, ст. 215.3 УК РФ). В этой связи предлагается в официальной статистической отчетности предусмотреть отдельно графу о состоянии преступности в области газовой промышленности, учитывая как нормативно-правовой, так и криминологический подходы.

2. При определении криминологических показателей преступности в области газовой промышленности следует акцент об удельном весе преступлений по степени тяжести (небольшой, средней тяжести, тяжкие и особо тяжкие), по формам и видам вины (умышленные и неосторожные), по видам мотивации (корыстные или легкомысленные), по субъектам преступления (мужчины, женщины, несовершеннолетние, безработные или должностные лица), по характеру и размерам причиненного вреда (ущерба) , а также с учетом «географию» такой преступности.

3. Учитывая тенденцию роста преступлений, совершенных с использованием электронной и информационно-телекоммуникационной сетей, а также в сфере компьютерной информации не стоит исключать, что в их объем также могут быть включены преступления в области газовой промышленности, поскольку при их совершении могут быть использованы различные аппаратные и (или) программно-аппаратные комплексы, облегчающие их совершение. Ярким примером этому служит распространенный в последнее время способ использования фальшивых квитанций для оплаты услуг поставки газа, которые вкладывают в почтовые ящики в жилище потерпевших или направляются в электронной форме по их электронной почте.

Список источников

1. Алексеев А.И. Криминология. Курс лекций. М.: Изд-во «Щит-М», 1998.

2. Криминология: Учебное пособие / под общ. ред. В.Е. Эминова. М.: Изд. группа ИНФРА-М; НОРМА, 1997.
3. Каиржанов Е. Криминология (общая часть). Алматы: Республиканский издательский кабинет, 1995.
4. Кудрявцев В.Н., Лунеев В.В. О криминологической классификации преступлений // Государство и право. 2005. № 6. С. 54-66.
5. Муслов Б.В. Латентная преступность: некоторые вопросы теории и практики противодействия: дис. … канд. юрид. наук. СПб, 2006.

А.Н. Колычева[1], **В.Ф. Васюков**[2]
[1]Орловский юридический институт МВД России
имени В.В. Лукьянова
[2]Московская академия Следственного комитета
имени А.Я. Сухарева

Маркетплейсы как инфраструктура незаконной наркоторговли в даркнете

Аннотация. Статья посвящена анализу маркетплейсов даркнета как специализированной инфраструктуры незаконного оборота наркотических средств и психоактивных веществ. На основе отечественных исследований и международного опыта показано, что даркнет-рынки функционируют не как случайные онлайн-площадки, а как сложные, самоорганизующиеся криминальные системы, имитирующие логистику, сервисы и бизнес-модели легальных электронных коммерческих платформ.

Ключевые слова: даркнет, маркетплейсы, незаконный оборот наркотиков, криптовалюты, эскроу, децентрализованные сети.

Цифровая эпоха кардинально изменила структуру нелегальных рынков. Традиционные схемы наркоторговли - через курьеров, почтовые рассылки, персональных диллеров всё чаще вытесняются онлайн-платформами, доступными лишь через специализированные сети. Одной из таких платформ стал «даркнет» (далее – даркнет) –

анонимная часть интернета, недоступная стандартным браузерам и поисковым системам. Об этом российскими исследователями упоминается в своих работах, посвященных противодействию киберпреступности[1].

Хотя даркнет изначально создавался не для противоправной деятельности, а для защиты права на приватность и свободу слова, он был адаптирован преступными группировками как среда для незаконной торговли. В отличие от открытого сегмента сети Интернет, где пользовательская активность может отслеживаться, даркнет обеспечивает практически полную анонимность как для продавцов, так и для покупателей[2].

Следует подчеркнуть, что термин «даркнет» (с англ. –*DarkNet*) представляет собой англоязычный неологизм, образованный путём слияния двух лексем: *dark* (тёмный) и *net* (сеть)3. Данный термин получил первоначальное распространение в научно-технической среде в 1970-х годах[4].

Между тем, историческое происхождение термина связано с необходимостью дифференциации компьютерных сетей, функционировавших в рамках проекта ARPANET (предшественника современного интернета), и изолированных сетей, не имевших прямого доступа к данной системе.

К слову, основной этап в развитии терминологического аппарата связан с публикацией научного исследования “The Darknet and the

---

[1] Саркисян А.Ж. Количественно-качественные показатели преступности в киберпространстве // Вестник Московского университета МВД России. 2024. № 3. С. 190-197; Саркисян А.Ж. Классификация и типология киберпреступников // Расследование преступлений: проблемы и пути их решения. 2024. № 4(46). С. 74-83; Саркисян А. Ж. Транснациональный характер преступности в киберпространстве // Расследование преступлений: проблемы и пути их решения. 2024. № 3(45). С. 71–75.

[2] Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие М.: Общество с ограниченной ответственностью "Проспект", 2025. 200 с.

[3] Поэтому *даркнет* в официальных источниках упоминается еще и как темная паутина, сеть, темный интернет и т.д.

[4] Баженова Е.Д. История и развитие Даркнета: от военных операций к нелегальной торговле // Управление регионом: тенденции, закономерности, проблемы : материалы III Международной научно-практической конференции, посвящённой Десятилетию науки и технологий в Российской Федерации: В 2-х частях, Горно-Алтайск, 20–21 июня 2024 года. Горно-Алтайск: Горно-Алтайский государственный университет, 2024. С. 52–54.

Future of Content Distribution” в 2002 году, подготовленного специалистами корпорации Microsoft. Именно эта работа способствовала популяризации термина в академическом сообществе1.

Подчеркнем, что в современной научной трактовке под термином «даркнет» принято понимать комплексную информационно-коммуникационную инфраструктуру, характеризующуюся особым набором технологических и функциональных параметров2. Ключевыми особенностями данной системы выступают наличие многоуровневых зашифрованных каналов передачи данных, реализация продвинутых механизмов анонимного информационного обмена, функционирование в качестве альтернативной коммуникационной платформы, а также обязательное использование специализированного программного обеспечения.

Изучение ряда отечественных исследований позволяет сказать, что даркнет как пространство преступной сети по незаконному распространению наркотиков представляет собой не просто технологическую нишу, а самоорганизующуюся криминальную систему3. В отличие от традиционных форм наркоторговли, основанной на иерархических цепочках поставок, даркнет-рынки трансформировали наркотический бизнес в децентрализованную, опосредованную сеть, где роль администраторов и продавцов переопределяется через алгоритмические механизмы, криптографическую защиту и криптовалютные транзакции.

---

[1] Biddle, Peter & England, Paul & Peinado, Marcus & Willman, Bryan. (2003) The Darknet and the Future of Content Distribution. URL: https://www.researchgate.net/publication/4820381_The_Darknet_and_the_Future_f_Content_Distribution.

[2] Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий / В.Ф. Васюков, К.К. Клевцов, В.И. Малик. Москва: Общество с ограниченной ответственностью "Издательство Прометей", 2023. 468 с.

[3] Преступления в сфере высоких технологий и информационной безопасности / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплыгина. Москва: Издательство Прометей, 2023. 1086 с.; Батраченко Д.А. Некоторые вопросы получения оперативно значимой и криминалистической информации из облачных хранилищ / Д.А. Батраченко, В.Ф. Васюков // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. № 1 (69). С. 98–107.

Маркетплейсы даркнета (с англ. - darknet marketplaces, DMs) представляют собой анонимные цифровые платформы, функционирующие исключительно в рамках защищённых сетей (например, Tor), которые стали ключевыми каналами легализации и распространения незаконных наркотических веществ на глобальном уровне. Используя криптовалюты как единственный механизм расчётов, эти платформы обеспечивают высокий уровень конфиденциальности для покупателей и продавцов, минимизируя риск выявления со стороны правоохранительных органов1.

Механизмы функционирования таких маркетплейсов основаны на сочетании децентрализованной архитектуры, сквозного шифрования, систем отзывов и рейтингов, а также модерации списков товаров с помощью администраторов и сообщества пользователей.

Такие наркотики как кокаин, метамфетамин, каннабис, синтетические опиоиды (например, фентанил) и новые психоактивные вещества (NPS), составляют подавляющую долю предлагаемых товаров – по оценкам, более 70–80% всех продаж на крупнейших маркетплейсах.

Платформы тёмной сети не ограничиваются простым предоставлением доступа к незаконным товарам; они функционируют как полноценные организационные системы, воспроизводящие логистические и сервисные механизмы легальных электронных рынков. В их структуру входят стандартизированные процедуры упаковки, скрытая транспортировка через почтовые и частные курьерские службы с использованием тактик маскировки - например, запутывание адресов, применение промежуточных пунктов пересылки - а также внедрение механизмов защиты покупателя, таких как система эскроу[2] и гарантии возврата средств при невыполнении обязательств по доставке. Такая организация формирует не просто канал сбыта, а устойчивый бизнес-модельный шаблон, имитирующий функциональность легитимных платформ

[1] Противодействие криптовалютным преступлениям в зарубежных странах / В.Ф. Васюков, А.Г. Волеводз, К.К. Клевцов [и др.]. Москва: Юрлитинформ, 2025. 504 с.

[2] Система «эскроу» (условное депонирование денежной суммы у третьего лица) используется на маркетплейсах в дарнете для защиты сделок, где уровень доверия между покупателями и продавцами низкий. Эскроу-сервисы (escrow services) выступают в роли гаранта, который собирает, хранит и выплачивает средства только в случае соблюдения условий сделки всеми сторонами.

электронной коммерции, но адаптированный под требования анонимности, риска и отсутствия правоприменительного контроля1.

Масштабы незаконной торговли, организуемой через эти платформы, достигают миллиардов долларов ежегодно. Даже после закрытия крупнейших рынков AlphaBay и Hansa, их функции быстро перенимаются новыми, часто более технологически продвинутыми платформами, демонстрируя высокую адаптивность и устойчивость преступной системы. Анализ транзакций показывает, что объёмы торговли сохраняются на стабильно высоком уровне, а география потребителей охватывает более 150 стран, включая страны Европы, Северной Америки, Австралии и Азии[2].

Значительную сложность представляет проблема должного реагирования в условиях цифровой анонимности. Современные маркетплейсы функционируют без центрального сервера, используют децентрализованные хостинги, а их администраторы часто находятся за пределами юрисдикции стран, где осуществляется наибольший спрос на наркотики. Что, собственно, порождает коллизии между национальными законодательствами, отсутствие единой практики экстрадиции и трудности в координации следственных действий[3].

Более того, усилия по закрытию платформ нередко приводят к эффекту «гидры» — при устранении одного узла возникают два новых, часто более устойчивых и скрытных.

В сложившейся ситуации эффективное противодействие наркоугрозе может осуществляться с учетом тщательно проработанных оперативных операций.

---

[1] Малик В.И. Отдельные меры противодействия незаконному обороту наркотических средств и психотропных веществ, совершаемому несовершеннолетними с использованием информационно-коммуникационных технологий // Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности : сборник статей. Орел, 28 октября 2022 года. Орёл: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2022. С. 43–46.

[2] Васюков В.Ф. Получение и использование абонентской информации при расследовании преступлений / В.Ф. Васюков, С.В. Расторопов, Д.Ф. Флоря. Орел: Картуш, 2025. 324 с.

[3] Малик В.И. Актуальные вопросы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационных технологий // Юридическое образование и наука. 2022. № 5. С. 35–39.

К примеру, во Франции агентурное внедрение, наблюдение, электронный перехват информации для выявления тяжких преступлениях, в том числе незаконного оборота наркотических средств, охватываются уголовно-процессуальным законом. Кроме того, во многих иностранных правоохранительных системах предпочтение отдается термину «специальные (или негласные) следственные действия» (например, ФРГ, Королевство Испания, Великобритания, США, Канада, КНР, Япония, КНДР, Республика Корея)[1].

Однако, несмотря на определенные успехи правоохранительных органов, борьба с преступными маркетплейсами остаётся сложной и устойчивой задачей из-за их высокой адаптивности, быстрой трансформации и зависимости от децентрализованных технологий: закрытие одной платформы почти неизбежно ведёт к возникновению новой. Эффективное противодействие требует координированного взаимодействия государственных структур, частного сектора кибербезопасности и международных организаций, направленного не только на оперативные пресечения, но и на системное разрушение экономических, коммуникационных и логистических цепочек, обеспечивающих функционирование этих платформ.

Список источников

1. Biddle, Peter & England, Paul & Peinado, Marcus & Willman, Bryan. (2003) The Darknet and the Future of Content Distribution. URL: https://www.researchgate.net/publication/4820381_The_Darknet_and_the_Future_ f_Content_Distribution.

2. Баженова Е.Д. История и развитие Даркнета: от военных операций к нелегальной торговле // Управление регионом: тенденции, закономерности, проблемы : материалы III Международной научно-практической конференции, посвящённой Десятилетию науки и технологий в Российской Федерации: В 2-х частях, Горно-Алтайск, 20–21 июня 2024 года. Горно-Алтайск: Горно-Алтайский государственный университет, 2024. С. 52–54.

[1] Малик В.И. Международно-правовые основы противодействия незаконному обороту наркотиков, совершаемому с использованием ИТТ / В.И. Малик, Д.Ф. Флоря // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 4(97). С. 246–253.

3. Батраченко Д.А. Некоторые вопросы получения оперативно значимой и криминалистической информации из облачных хранилищ / Д.А. Батраченко, В.Ф. Васюков // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2025. № 1 (69). С. 98–107.

4. Васюков В.Ф. Получение и использование абонентской информации при расследовании преступлений / В.Ф. Васюков, С.В. Расторопов, Д.Ф. Флоря. Орел: Картуш, 2025. 324 с.

5. Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие М.: Проспект, 2025. 200 с.

6. Малик В.И. Актуальные вопросы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационных технологий / В. И. Малик // Юридическое образование и наука. 2022. № 5. С. 35–39.

7. [1]Малик В.И. Международно-правовые основы противодействия незаконному обороту наркотиков, совершаемому с использованием ИТТ / В. И. Малик, Д. Ф. Флоря // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 4(97). С. 246–253.

8. Малик В.И. Отдельные меры противодействия незаконному обороту наркотических средств и психотропных веществ, совершаемому несовершеннолетними с использованием информационно-коммуникационных технологий // Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности : сборник статей. Орел, 28 октября 2022 года. Орёл: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2022. С. 43–46.

9. Преступления в сфере высоких технологий и информационной безопасности / В.Ф. Васюков, А.Г. Волеводз, М.М. Долгиева, В.Н. Чаплыгина. Москва: Издательство Прометей, 2023. 1086 с.

10. Противодействие криптовалютным преступлениям в зарубежных странах / В.Ф. Васюков, А.Г. Волеводз, К.К. Клевцов [и др.]. Москва: Юрлитинформ, 2025. 504 с.

11. Противодействие преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием информационно-телекоммуникационных технологий / В.Ф. Васюков, К.К. Клевцов, В.И. Малик. Москва: Издательство Прометей, 2023. 468 с.

12. Саркисян А. Ж. Транснациональный характер преступности в киберпространстве // Расследование преступлений: проблемы и пути их решения. 2024. № 3(45). С. 71–75.
13. Саркисян А.Ж. Классификация и типология киберпреступников // Расследование преступлений: проблемы и пути их решения. 2024. № 4(46). С. 74–83.
14. Саркисян А.Ж. Количественно-качественные показатели преступности в киберпространстве // Вестник Московского университета МВД России. 2024. № 3. С. 190–197.

В.Н. Карагодин
Московская академия Следственного комитета
имени А.Я. Сухарева

Основные элементы методики расследования киберпреступлений экстремистской направленности, совершаемых несовершеннолетними

Аннотация. В концептуальных основах методики рассматриваются особенности киберпреступлений несовершеннолетних, с учетом которых выделяются основные элементы расследования данного вида посягательств.

Ключевые слова: киберэкстремизм, несовершеннолетние, криминалистическая характеристика, ситуации расследования.

К основным элементам любой частной криминалистической методики, прежде всего, относится учет своеобразия вида или группы преступлений, для расследования которых она создается.

В теории криминалистики для учета упомянутой специфики используется такая научная категория как криминалистическая характеристика преступлений[1].

К основным особенностям преступлений рассматриваемого вида относятся типичные свойства личности несовершеннолетних субъектов. Среди них должна быть выделена степень устойчивости антиобщественной направленности указанных лиц. По этому

[1] Бессонов А.А. Криминалистическая характеристика преступлений // Криминалистика: учебник. В 3-х ч. Часть 3. Криминалистическая методика / Под ред. В.В. Бычкова, С.В. Харченко, Москва, 2021. С. 16–17.

основанию могут быть выделены субъекты с устойчивыми представлениями о возможности и необходимости пропаганды национальной, религиозной и иной ненависти, применения насилия в отношении представителей разных социальных групп, представляющих собой объект вражды или ненависти по указанным мотивам. Субъекты с такими взглядами это в основном подростки 16-17-летнего возраста, твердо не только убежденные в допустимости названных представлений, но и неоднократно руководствующиеся ими в процессе распространения и практической реализации.

К подросткам с установкой экстремистской направленности средней степени выраженности относятся несовершеннолетние, полагающие допустимыми пропаганду указанных взглядов и насилия на почве ненависти к представителям отдельных национальных, религиозных и иных групп в отдельных ситуациях.

Некоторые из таких субъектов испытывают так называемую борьбу мотивов принятия решений о совершении преступлений данного вида.

Наконец, существуют субъекты данного вида преступлений, осознающие общественную опасность и противоправность, но безразлично относящиеся к этому.

Например, юноша, призывавший через электронные сети подростков принять участие в избиении в установленном месте представителей национальной диаспоры, заявил, что ему хотелось поучаствовать в групповой драке. По его словам, он уже несколько раз принимал участие в таких драках в составе группы фанатов и ему понравились испытываемые при этом ощущения. Прочитав в сетях сообщения о готовящемся столкновении, он передал его нескольким другим членам фан-клуба. При этом он понимал, что совершает противоправное деяние, призывая к насилию в отношении представителей этнической группы, ведущих себя враждебно по отношению к русскоязычному населению.

В научной литературе отмечалось, что значительное количество преступлений рассматриваемого вида совершается несовершеннолетними в составе неформальных группировок экстремистско-националистической направленности[1].

К этому нужно добавить, что определенная часть таких преступлений совершаются несовершеннолетними в одиночку.

---

[1] Бычков В.В. Противодействие преступлениям экстремистской направленности. М., 2013. С. 64.

Необходимо также заметить, что несовершеннолетние могут самостоятельно создавать и готовить к распространению с использованием цифровых технологий экстремистские материалы.

Текст таких материалов и внешнее оформление могут заимствоваться из уже размещавшихся в электронных сетях и других источниках. Реже подростки в одиночку формируют подобные материалы. Представляется, что составляемые таким образом тексты, печатные воззвания, видео и аудиоклипы отличаются простотой, а в ряде случаев примитивностью, поскольку их изготовители не обладают ни требуемыми для этого умениями, ни знаниями и оборудованием.

При создании названных материалов группами могут использоваться сценарии, заготовки, специально подготовленные для несовершеннолетних взрослыми организаторами, подстрекателями. Личность таких взрослых субъектов может быть известна только нескольким руководителям группы несовершеннолетних.

Изготовители могут разрабатывать материалы, подлежащие распространению среди неопределенного или ограниченного определенными параметрами круга лиц. В частности, известны случаи подготовки и распространения через электронные сети призывов несовершеннолетних к актам насилия в отношении представителей определенных национальных, религиозных, иных социальных групп.

При самостоятельном создании экстремистских материалов, в особенности четкой адресной направленности, более полно отражается свойства личности несовершеннолетних авторов текстов, видео, аудиоматериалов. Это могут быть, прежде всего, признаки письменной речи. Аналогичным образом отражаются свойства личности авторов сценариев, заготовок, послуживших основой для создания на их основе экстремистских материалов.

В коллективно создаваемых материалах отражаются свойства личности нескольких авторов, а также изготовителей. Признаки этих свойств позволяют создавать профили отдельных участников, а также группы в целом.

Уместно заметить, что кроме материалов, содержащих исключительно призывы вышеупомянутого характера, могут распространяться тексты, изображения, направленные на вовлечение несовершеннолетних в экстремистскую деятельность. Это могут быть открытые приглашения к посещению мероприятий, запрещенных или

не выявленных правоохранительными учреждениями экстремистских организации.

Иногда содержание таких материалов довольно тщательно маскируются под тексты, клипы, фильмы, содержание которых не имеет ничего общего с пропагандой ненависти, вражды, призывами к насилию и иной экстремистской деятельности.

Такие носители информации нередко изготавливаются на профессиональном уровне с использованием высокотехнологичного оборудования. Часть такой продукции производится за рубежом, затем полностью или частично переправляются в нашу страну посредниками или непосредственным распространителями.

В мотивах некоторых распространителей доминирующее значение приобретает стремление к самоутверждению, потребность к необычным занятиям, осуществлению конспиративной деятельности, да еще и запрещенной законом. Естественно, что реализация этих желаний связывается с удовлетворением потребности в получении острых ощущений от распространения экстремистских материалов.

Несовершеннолетние распространители из числа участников экстремистских групп нередко испытывают положительные эмоции от ощущения принадлежности к криминальному объединению, сопричастности к политической деятельности.

Эти особенности оказывают влияние на способы преступлений рассматриваемого вида. В большинстве своем они являются полноструктурными, то есть охватывающими действия по подготовке, непосредственному совершению и сокрытию преступления.

Особенностью этих способов является реализация отдельных элементов на разных территориях и отражение в их содержании свойств личности именно несовершеннолетних субъектов. Среди последних могут быть названы повышенная эмоциональность, использование лексических и стилистических средств, присущих подросткам, проживающим на определенных территориях, принадлежащих к определенным группам, обладающих набором определенных знаний, умений формирования анализируемых материалов, использования определенного программного оборудования, продукта, возможность применения для изготовления и распространения конкретных технических средств.

Представляется, что при формировании частных криминалистических методик следует выделять типичные свойства

личности несовершеннолетних субъектов, относящихся к разным возрастным группам, исполняющих разные роли в преступной деятельности. Соответственно этому должны обобщаться типовые способы преступлений, реализуемых несовершеннолетними субъектами, принадлежащими к разным классификационным группам.

Конечно же необходимо выявление типичных свойств реализации типовых способов представителями разных классификационных групп несовершеннолетних.

Своеобразием отличается и поведение несовершеннолетних субъектов преступлений данной группы в ходе расследования. Для некоторых характерно оказание упорного противодействия расследованию, несмотря на предъявление не просто убедительных, а порой неопровержимых доказательств.

Можно предполагать, что для несовершеннолетних с устойчивой экстремистской направленностью личности характерно сокрытие соучастников и их ролей. Некоторые из таких субъектов не только признают свою вину в реально совершенных деяниях, но и оговаривают себя.

С учетом изложенного в рекомендациях по раскрытию преступлений экстремистской направленности, совершенных несовершеннолетними, могут быть выделены научно обоснованные предложения по установлению причастности к такого рода деяниям лиц, не достигших совершеннолетия.

В ситуациях обнаружения фактов распространения в электронных сетях призывов к совершению конкретных насильственных актов на почве вражды и ненависти к представителям определенных групп, а также других материалов экстремистского характера, должны проверяться версии о причастности к таким деяниям несовершеннолетних. Основаниями для выдвижения таких версий являются данные о типичных и индивидуальных свойствах личности несовершеннолетних субъектов, отразившихся как в содержании распространяемых материалов, так и в действиях по их распространению.

Достаточно сложной и важной задачей на данном этапе является определение пространственных границ поиска несовершеннолетних субъектов такого рода деяний. Некоторые из них используют технические средства, методы и приемы сокрытия места своего пребывания. В подобных ситуациях возможно проведение

специальных оперативно-разыскных мероприятий, предполагающих установление прямых контактов с предполагаемыми субъектами преступления путем переписки, проведения личных встреч с ними и т.п.

В ряде ситуаций в распространяемых материалах имеются данные о возможном пребывании разыскиваемых в конкретном населенном пункте, микрорайоне, обучении в определенном учебном заведении, о принадлежности к известным объединениям по увлечениям в свободное время, по профессиональной деятельности, этнической, религиозной принадлежности.

Представляется, что назрела необходимость разработки методик психолингвистических, компьютерно-технических исследований названных материалов для проверки версии о возможном совершении выявленного преступления данного вида несовершеннолетними.

Несомненно, требуются и криминалистические рекомендации по построению, проверки версий о совершении несовершеннолетними преступлений рассматриваемого вида.

Как известно, в сложных проблемных ситуациях первоначально выдвигаются и проверяются версии о принадлежности несовершеннолетнего к определенной группе лиц, дислоцирующихся на конкретной территории. После установления состава группы выясняется, кто из ее членов обладает свойствами личности, отразившимися в способе расследуемого преступления и следах его реализации.

Поскольку речь идет о преступлениях, совершаемых с использованием современных цифровых технологий, важное значение имеет подготовка рекомендаций по установлению признаков использования конкретных программных средств и персональных компьютеров для изготовления и распространения экстремистских материалов[1]. Не менее важным моментом является доказывание использования именно проверяемым несовершеннолетним вышеуказанных средств.

Одновременно важно ввести целенаправленную поисковую деятельность по установлению соучастников предполагаемого субъекта преступления. Она также требует организации взаимодействия следователя с сотрудниками органов дознания,

[1] Льянов М.М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической деятельности в сети Интернет. Автореф. дис. … канд. юрид. наук. Екатеринбург, 2015. С. 19–25.

специалистами в области подростковой психологии, другими лицами, способными оказать содействие в решении задач досудебного производства.

Несовершеннолетних субъектов рекомендуется задерживать одновременно с другими, по крайней мере, основными участниками группы, чтобы не только пресечь ее деятельность, но и предотвратить возможное сокрытие содеянного. В этих целях необходимо проведение групповых обысков, осмотров мест происшествия, средств компьютерной техники, использованной для совершения преступления, допросов задержанных, проведение их психологического исследования и т.п.

Проверка обоснованности подозрений несовершеннолетних предполагает проведение комплекса следственных действий (тактических операций), включая допросы подозреваемых, проведение экспертиз для идентификации их в качестве изготовителей экстремистских материалов, пользователей конкретными средствами распространения и т.п.

Представляется, что решение этой задачи целесообразно осуществлять с использованием фактора внезапности и в максимально сжатые сроки.

На последующих этапах расследования решаются задачи: предъявление и проверка обоснованности обвинения несовершеннолетнего в преступлениях данного вида, выявление всех участников деяния и их ролей, установление обстоятельств, способствовавших совершению посягательств.

Необходимо подчеркнуть, что при расследовании данного вида преступления осуществляется важнейшая воспитательная функция, заключающаяся в изменении взглядов несовершеннолетних на допустимость содеянного.

Список источников

1. Бессонов А.А. Криминалистическая характеристика преступлений // Криминалистика: учебник. В 3-х ч. Часть 3. Криминалистическая методика / Под ред. В.В. Бычкова, С.В. Харченко. Москва, 2021.

2. Бычков В.В. Противодействие преступлениям экстремистской направленности. М., 2013. 254 с.

3. Льянов М.М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической деятельности в сети Интернет. Автореф. дис. … канд. юрид. наук. Екатеринбург, 2015. 25 с.

А.А. Лебедева
Московская академия Следственного комитета
имени А.Я. Сухарева

Установление связи между лицом и цифровой валютой

Аннотация. В статье рассматриваются следственные ситуации по преступлениям, совершаемым с использованием цифровой валютой в России. Обозначены направления установления связи между лицом и цифровой валютой. Приведены доводы ученых, а также следственная и судебная практика

Ключевые слова: цифровая валюта, расследование, установление владельца, криминалистика.

Цифровая валюта (далее по тексту ЦВ) — это группа валют, к которой относятся все виртуальные валюты, стейблкоины и Цифровая валюта центрального банка[1].

Виртуальные валюты включают криптовалюту, игровые токены или другие типы токенов.

Криптовалюты – это виртуальные валюты, которые используют криптографические методы. Таким образом понятие ЦВ «поглощает» понятие криптовалюта.

Самыми распространенными преступлениями, совершаемыми с использованием ЦВ в России, как и в других государствах, являются незаконный сбыт наркотических средств, легализация (отмывание)

[1] См.: Федеральный закон от 31.07.2020 г. № 259-ФЗ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации; Положение Банка России от 03.08.2023 N 820-П (ред. от 12.07.2024) «О платформе цифрового рубля» (вместе с Порядком урегулирования споров и разногласий, зарегистрировано в Минюсте России 10.08.2023 № 74716) (с изм. и доп., вступ. в силу с 01.01.2025).

преступных доходов, мошенничество и деяния коррупционной направленности[1].

Успех расследования преступлений рассматриваемой категории зависит от слаженного и грамотного взаимодействия следователя, сотрудников оперативных подразделений, представителей Федеральной службы по финансовому мониторингу (далее – Росфинмониторингом), а также квалифицированного специалиста в области информационно-коммуникационных технологий.

При расследовании преступлений рассматриваемой категории представляется возможным выделить следующие исходные следственные ситуации:

1. Имеется информация, содержащая данные идентификатора криптокошелька.

Так, в ходе предварительного расследования установлено, что 15.11.2019 в 18 часов 54 минуты свидетель К., в пользовании которого находится криптокошелек, имеющий адрес: TYxE1C6CrmnGhZB3RvweXFwrngdgnytJhh, получил перевод ЦВ в размере 152 806 TRX, которая ранее была похищена с криптокошелька, принадлежащего Ж.

2. Имеется информация, что у подозреваемого/обвиняемого в совершении преступления по уголовному делу имеется ЦВ. Указанная ситуация может быть представлена в следующих вариациях:

2.1. Имеется информация, что у подозреваемый/обвиняемый в совершении преступления получил взятку в ЦВ.

2.2. Имеется информация, что у подозреваемый/обвиняемый в совершении преступления в качестве вознаграждения за совершения незаконных действий (убийство по найму, реализацию наркотических средств и психотропных веществ и др.) получил вознаграждение в ЦВ.

В первой исходной следственной ситуации: имеется информация, содержащая данные идентификатора криптокошелька. Алгоритм действия следователя будет направлен на установление личности преступника «от идентификатора криптокошелька к личности преступника».

---

[1] Тисен О.Н. Механизм совершения преступлений с использованием криптовалют: по результатам анализа следственной и судебной практики // Российский следователь. 2024. № 5. С. 7–11.

Блокчейн – один из вариантов реализации сети распределенных реестров, в котором данные структурируются в виде цепи (последовательности) криптографически связанных блоков транзакций. Каждый последующий блок содержит зашифрованную информацию из предыдущего блока, чтобы обеспечивать последовательность и неизменность записей[1]. Является технологической основой ЦВ и их обращения.

Транзакция – это процесс перевода определенного количества ЦВ от одного владельца другому. В общем случае основное содержание транзакции составляют два списка – список входов, каждый из которых состоит из ID транзакции, номера выхода, сценария разблокировки (как правило, открытый ключ и электронная подпись отправителя/владельца), и список выходов, каждый из которых состоит из данных о сумме перевода и условии вывода средств (как правило, адрес получателя платежа).

ID транзакции (TXID) – это 64-символьный код, состоящий из определённой последовательности букв и цифр. Он генерируется индивидуально для каждой транзакции и содержит информацию о ней, но в то же время является общедоступным.

Адрес криптовалюты (идентификатор криптокошелька) – это точка нахождения токенов в блокчейне, необходимая для хранения ЦВ и последующих финансовых операций. Генерируется случайным образом и состоит из латинских букв и цифр. Точное количество символов зависит от типа кошелька, а точнее, от того, к какой ЦВ привязан.

[1] Основные направления развития финансовых технологий на период 2025–2027 годов (одобрены Советом директоров Банка России) / Текст документа приведен в соответствии с публикацией на сайте https://www.cbr.ru/ по состоянию на 15.10.2024.

Адрес криптовалюты (идентификатор криптокошелька)

ЦВ	Особенности адреса	Пример
TRON Tronix (TRX)	имеют одинаковую длину в 42 символа и начинаются с буквы «T»,	*TPAe77oEGDLXuNjJhTyYeo5vMqLYdE3GN8U*
Ethereum (ETH)	имеет длину от 40 до 44 символов, всегда начинается с «0x».	*0x690B9A9E9aa1C9dB991C7721a92d351Db4FaC990*
Ripple (XRP)	начинается с 'r'	*r34v7y6d54q37654321*
Bitcoin	Комбинация цифр и прописных и строчных букв латинского алфавита. Длинна от 26 до 36. В большинстве -34. Не используются заглавная буква O, I, строчная буква l и число 0, Адрес всегда начинается с 1, 3 или bc1.	Legacy (Pay-to-Pub) (P2PKH), начинается с 1: *1njrRcKQtfjjLuQxFYCeMXcth77m5TAYo*
		Scrypt (P2SH) адрес, начинается с 3 : *3HYLqq5JRbWeP54MmkTb5r2KuHifWAqLnv*
		SegWit Bech32, начинается с bc1 *bc1q8ctmys2mzqjrsztxlv7pe9s5azh9acrvg9jpmy* *bc1peu5hzzyj8cnqm05le6ag7uwry0ysmtf3v4uuxv3v8hqhvsatca8ss2vuwx*

Информация о владельце ЦВ, по мнению О.Н. Тисен[1] и других авторов[2], может быть получена путем направления поручения в соответствии с нормами УПК РФ оперативным сотрудникам с целью установления сведений, идентифицирующих предполагаемого

[1] См.: Тисен О.Н. Специфика расследования преступлений, совершенных с использованием криптовалют // Особенности противодействия гибридным угрозам в отношении Российской Федерации: Материалы Луганского международного юридического форума, Луганск, 14 мая 2024 года. Луганск: Луганская академия Следственного комитета, 2024. С. 166–178.

[2] См.: Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография / под ред. Е.В. Емельяновой и О.С. Бутенко. СПб: Санкт-Петербургская академия СК России, 2022. 250 с.

преступника, его потенциальных сообщников, в том числе идентификатора криптокошельков, логинов учетных записей на интернет-ресурсах провайдеров услуг в сфере виртуальных активов, USER-агентов (пользователей) использованных Интернет-браузеров, IP-адресов, электронных почтовых ящиков и иной значимой информации, в том числе при использовании данных, полученные из так называемых «открытых источников информации», в том числе из сети Интернет (социальные сети, форумы)[1];

- при направлении в соответствии с нормами УПК РФ запросов *провайдерам услуг в сфере виртуальных активов* (далее по тексту - ПУВА)[2]. К числу ПУВА относятся криптобиржи и криптообменники.

ПУВА, действующие на так называемой «легальной» основе, осуществляют свою деятельность на основании принципов AML[3] и процедуры KYC[4] (Know Your Customer / Знай своего клиента)

Процедура «Знай своего клиента» условно подразделяется на три этапа. Первый называется «Программа идентификации клиентов» - происходит сбор данных о так называемом клиенте ПУВА и их первоначальная проверка. Вторая стадия — «Комплексная проверка клиентов» - осуществляется более тщательное исследование информации о клиенте, на предмет его причастности к противоправной деятельности. Третья стадия — «Постоянный мониторинг», в ходе которой актуализируется информация, полученная на первых двух стадиях, а также выявляют различные

---

[1] См.: Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды академии МВД России. 2021, № 4 (60). С. 101-108.

[2] ПУВА – физические или юридические лица, осуществляющие в качестве предпринимательской деятельности один или более следующих видов операций для/или от имени другого физического или юридического лица: обмен между ЦВ и фиатными валютами; обмен между одной или более формами ЦВ; перевод ЦВ; хранение и/или администрирование ЦВ или инструментов, позволяющих осуществлять контроль над ЦВ; участие и предоставление финансовых услуг, связанных с предложением выпускающего лица и/или продажей ЦВ.

[3] Принципы AML – подразумевают действия ПУВА по установлению, хранению и обмене информацией о подозрительных транзакциях между уполномоченными органами, а также принятию мер к их замораживанию (блокировке).

[4] KYC (*Know Your Customer* / Знай своего клиента)- принцип деятельности ПУВА, основанный на необходимости обязательной идентификации лиц, пользующихся услугами ПУВА.

подозрительные операции, в том числе свидетельствующие о причастности лица к «финансированию терроризма».

Во второй исходной следственной ситуации- имеется информация, что у подозреваемого/обвиняемого в совершении преступления по уголовному делу имеется ЦВ – алгоритм следственных действий будет направлен на отыскание находящегося во владении фигуранта уголовного дела криптокошелька с ЦВ на его персональном компьютере (далее по тексту – ПК), смартфоне и иных электронных носителях информации, а также установлении обстоятельств, указывающих непосредственно на принадлежность ЦВ именно ему.

- Наличие ЦВ у подозреваемых возможно выявить путем таких процессуальных действий как осмотр или обыск за исключением случаев, когда холодный криптокошелек представляет собой физический лист бумаги, на котором записаны закрытые и открытые ключи, как правило, в виде QR-кода.

Файлы и документы в ходе проведения осмотра содержимого ПК можно осуществлять при помощи встроенного функционала операционных систем (встроенная система поиска в файловой системе), либо специализированных программ, таких как «Архивариус 3000», «Ищейка проф Deluxe» и другие аналоги. Вместе с тем, для того чтобы выявить файлы, в которых содержатся строки, содержащие ключи криптокошельков необходимо для поиска ввести последовательность символов в точности, повторяющих ключ криптокошелька.

– производство в соответствии с нормами УПК РФ осмотров с привлечением специалиста и использованием Интернет-браузеров ПК и смартфонов фигурантов уголовного дела с целью отыскания, используемых злоумышленником криптокошельков, логинов учетных записей, например, на таких Интернет-ресурсах как bitcointalk.org, blockchain.com, walletexplorer.com[1] (позволяет идентифицировать принадлежность биткоин-кошельков конкретным компаниям);

В ходе следственных следствий, направленных на отыскание и изъятие материальных объектов и цифровых следов (осмотр, обыск, выемка), следует обращать особое внимание на электронные и непосредственные записи, содержащие такие криминалистически значимые сведения, как bitcoin-адреса, записанные на бумажный или

[1] walletexplorer.com – интернет-ресурс, который позволяет идентифицировать принадлежность биткоин-кошельков конкретным компаниям

электронный носитель ключи. Такой поиск может вестись на ПК и смартфонах с целью обнаружения стандартных форматов программных криптокошельков, анализа оперативной памяти или выгрузки необходимых сведений с работающего устройства (например, если в момент внезапного начала обыска осуществлялась и не была прервана работа с криптокошельком).

Сведения о криптокошельках могут сохраниться в служебных журналах системных и прикладных программ, программах-кошельках, используемых для осуществления транзакций, а также файлах *wallet.dat.*

Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РФ порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства.

Принадлежность ЦВ лицу (кругу лиц, исходя из следственной и судебной практик), устанавливается на основании следующих фактов:

– владение приватным ключом доступа к криптовалютному кошельку, позволяющему совершать операции с находящейся в нем ЦВ;

Так, в ходе производства экспертизы и предметов: ноутбука марки Apple" "MacBook Pro" модель "A 1708", изъятого при производстве обыска в жилище ФИО1; моноблока марки "Apple" модель "A 2438", изъятого при производстве обыска в служебном кабинете N; при просмотре сведений, имеющихся во вкладке "Приложения", "Apple Notes" обнаружена заметка с характеристиками: название - "Пенсия" с приложением двух фотографии: на первой фотографии имеется рукописная запись из 8 цифр следующего содержания "24562456", в нижней части листа имеются рукописные записи, всего в 24 слова на иностранном языке, которые записаны в 2 колонки, а также рукописная запись "2", которая обведена кругом; на второй фотографии имеется рукописная запись из 8 цифр следующего содержания "65426542", в нижней части листа имеются рукописные записи, всего в 24 слова на иностранном языке, а также рукописная запись "1", которая обведена кругом.

Согласно протоколу осмотра, двух фотографии, распечатанных в ходе осмотра предметов, со слов участвующего в осмотре специалиста ФИО16 фразы на фотографиях, вероятно, являются SEED-фразами, которые предназначены для резервного доступа к криптокошельку, для чего необходимо их ввести в устройство фирмы "Ledger", для чего

использовался для осмотра аппаратный кошелек для криптовалют "Ledger Nano X". Со слов специалиста ФИО16 факт получения доступа к криптокошельку указывает на его принадлежность ФИО1, у которого были изъяты SEED-фразы, и позволяют ФИО1 владеть, пользоваться и распоряжаться имеющейся криптовалютой[1].

– указание адреса криптовалютного кошелька для приема платежей на странице в социальной сети, в переписке посредством сервиса мгновенных сообщений (мессенджеров), записи в блоге, сообщении на форуме или на сайте;

Следует помнить, что отслеживание транзакций не всегда приводит к точной идентификации личности владельца кошелька. Криптовалютные кошельки не содержат личной информации, и для того, чтобы связать адрес с конкретным человеком, необходимы дополнительные данные – например, информация от ПУВА, где кошелек был использован для регистрации.

– указание сведений о личности в соответствии с правилами функционирования ПУВА[2].

Так, Т. действуя группой лиц по предварительному сговору с Л., используя реализуя свой преступный умысел, направленный на легализацию денежных средств, полученных от неустановленного лица под аккаунтом «ММ», зарегистрированном в приложении «в сети Интернет, за незаконную деятельность, связанную с незаконным сбытом наркотических средств в виде ЦВ «Биткойн», зарегистрировала на сайте «свой электронный кошелек, имеющий буквенно-цифровой код, относящийся к числу неперсонифицированных, получив возможность анонимно отправлять и получать денежные средства, хранить и моментально обменивать ЦВ, управлять своими средствами, полученными в результате совершения незаконного сбыта наркотических средств[3].

[1] Определение Второго кассационного суда общей юрисдикции от 13.02.2024 по делу № 88-1886/2024, 88-36184/2023 (УИД 77RS0018-02-2023-001858-50)

[2]Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды академии МВД России. 2021, № 4 (60). С. 101-108.

[3] Приговор Волгодонского районного суда Ростовской области от 23.12. 2021 (УИД 61RS0012-01-2021-006159-08 дело №1-470/2021).

Список источников

1. Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды академии МВД России. 2021, № 4 (60). С. 101–108.
2. Особенности расследования преступлений, совершаемых с использованием цифровой валюты: монография / под ред. Е.В. Емельяновой и О.С. Бутенко. СПб: Санкт-Петербургская академия СК России, 2022. – 250 с.
3. Тисен О.Н. Специфика расследования преступлений, совершенных с использованием криптовалют // Особенности противодействия гибридным угрозам в отношении Российской Федерации: Материалы Луганского международного юридического форума, Луганск, 14 мая 2024 года. Луганск: Луганская академия Следственного комитета Российской Федерации, 2024. С. 166–178.
4. Тисен О.Н. Механизм совершения преступлений с использованием криптовалют: по результатам анализа следственной и судебной практики // Российский следователь. 2024. № 5. С. 7–11.

П.А. Литвишко
Генеральная прокуратура Российской Федерации

Международно-правовые аспекты противодействия киберэкстремизму в свете научного наследия В.В. Бычкова

Аннотация. Статья посвящена проблемам международного сотрудничества в противодействии киберэкстремизму. Освещается вклад В.В. Бычкова в науку и практику по этой теме, в частности, в контексте Конвенции ООН против киберпреступности. Показана роль прокуратуры РФ в этой области.

Ключевые слова: В.В. Бычков, киберэкстремизм, международное сотрудничество, Конвенция ООН против киберпреступности, прокуратура России.

«Теория и практика расследования преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей» – успешная и не успевшая к защите

докторская, теоретически фундаментальный и одновременно прикладной, востребованный практикой, новый и актуальный труд по противодействию киберэкстремизму[1]. Как и все, что создавал Василий Васильевич Бычков. Всем известным мне его исследованиям так или иначе свойственны масштабность, глубина проработки избранной темы, подлинная погруженность в нее автора, его нацеленность на созидание нового и при этом добросовестное исчерпание в работе всех имевшихся до него источников по теме (как правило, включавших в себя и материалы в области международного права), что неизменно гарантировало его богатый и качественный интеллектуальный вклад в науку и практику, как отечественную, так и международную. Если же говорить о широте диапазона научных интересов, разносторонности Василия Васильевича, то здесь тоже мало сыщется равных ему: вряд ли найдется современная и актуальная для уголовного права, процесса, криминалистики тема, которая осталась бы не охваченной в той или иной мере его работами.

---

[1] По определению В.В. Бычкова, киберэкстремизм – это «системно организованные, целенаправленные, общественно опасные, сознательно совершаемые информационные индивидуальные или групповые атаки на сознание и психику неограниченного количества пользователей социальных сетей и других современных средств электронной информации, совершаемые с использованием компьютеризованных устройств, современных информационных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет, с целью возбуждения общественно опасных политических, идеологических, расовых, национальных, религиозных ненависти или вражды, а также ненависти или вражды в отношении какой-либо социальной группы, сопровождаемые соответствующими организационными, техническими и финансовыми мерами, запрещенные рядом уголовно-правовых норм Особенной части Уголовного кодекса РФ». См.: Бычков В.В. Теория и практика расследования преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей: дис. … д-ра юрид. наук. М., 2023 (неопубликованная рукопись). С. 16, 78, 128–129, 493, 496–497.

Впоследствии основной текст этой рукописи воспроизведен в издании: Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д. ю. н., д. т. н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. 572 с.

См. также: Прорвич В.А. Научные и организационные основы государственной программы борьбы с киберэкстремизмом: творческое наследие Василия Васильевича Бычкова // Расследование преступлений: проблемы и пути их решения. 2024. № 1. С. 187–198.

Непосредственно по проблематике экстремизма в его аналоговой и цифровой ипостасях им опубликовано большое число не только статей, но и объемных книг.

Нельзя не вспомнить и о других уникальных личных качествах Василия Васильевича: думаю, без исключения каждому, кому довелось быть знакомым с ним, становилось ясно сразу – перед вами порядочный, доброжелательный, профессиональный и при этом скромный человек.

Сказанное выше, безусловно, предопределило и выбор им упомянутой темы докторской диссертации, заключающей в себе двойную актуальность и добавленную стоимость: злободневность проблемы экстремизма в текущих геополитических реалиях[1] и повсеместная виртуализация человеческой жизнедеятельности, включая преступность, самоочевидны. В то же время ей не может быть приписана конъюнктурность, она имеет непреходящее значение для настоящего и будущих поколений, ведь, как известно, побороть явление экстремизма, как и преступности в целом, нельзя, ему возможно на постоянной основе противодействовать, равно как необратима и его виртуализация.

Ну и, конечно же, самому человеконенавистническому, дегуманизирующему, разрушительному и антигосударственному

[1] Согласно информации, подготовленной в Генеральной прокуратуре РФ во исполнение приказа Генерального прокурора РФ от 21.03.2018 № 156 «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности», в 2024 г. на рассмотрении в Генеральной прокуратуре РФ по уголовным делам о преступлениях экстремистской направленности находилось 11 запросов компетентных органов иностранных государств о выдаче лиц для уголовного преследования или исполнения приговора; в компетентные органы иностранных государств направлен 1 запрос о выдаче лица и 2 запроса о задержании. В компетентные органы иностранных государств направлено 7 запросов правоохранительных органов Российской Федерации об оказании правовой помощи по уголовным делам о преступлениях экстремистской направленности (2 – в Сирию, по 1 – в Азербайджан, Гонконг, Ирак, США, Эстонию), в Генеральную прокуратуру РФ поступили 84 запроса компетентных органов иностранных государств (70 – из Таджикистана, 11 – из Белоруссии, по 1 – из Азербайджана, Словакии и Южной Осетии). Из Генеральной прокуратуры Республики Таджикистан в Генеральную прокуратуру РФ поступил один запрос об осуществлении уголовного преследования в отношении российского гражданина. Исполнен один ранее поступивший запрос компетентного органа Таджикистана об оказании правоохранительного содействия по уголовному делу.

существу этого социального зла были противопоставлены человечная, созидательная натура и патриотизм его исследователя.

Одновременно Василий Васильевич предостерегал от сугубо «технократических» подходов в уголовном судопроизводстве, «создающих реальную угрозу превращения правового поля в площадку для игр компьютерных роботов»[1].

В 2023 г. нам в Генеральной прокуратуре выпала честь участвовать во внедрении в практическую деятельность положений докторской диссертации В.В. Бычкова по линии профильного управления по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму, а также Университета прокуратуры РФ, ими были изданы акты внедрения. Работа ожидаемо получила высокие отзывы.

С Василием Васильевичем мы познакомились за десять лет до этого в мае 2013 г. при подготовке конференции в тогда еще ИПК СК России и потом всегда поддерживали связь; в том же 2013 г. была издана его первая монография по экстремизму[2]; на следующий год он лично инициативно пришел поддержать защиту мной кандидатской в МГЮА, а еще через год вместе с единомышленниками организовал первую международную конференцию Академии СК России по теме противодействия экстремистским преступлениям, опубликовал две статьи в ее сборнике (в ту пору еще без приставки «кибер»)[3]. В последний раз мы увиделись через те же десять лет в конце апреля 2023 г. на конференции по киберпреступности в Академии, где

---

[1] Бычков В.В. Теория и практика расследования преступлений экстремистской направленности... С. 348, 364, 508.

[2] Бычков В.В. Противодействие преступлениям экстремистской направленности. М.: Юрлитинформ, 2013. 256 с.

[3] Бычков В.В. Особенности производства допросов при расследовании преступлений экстремистской направленности; Бычков В.В., Литвишко П.А. Идентификация по татуировкам участников уголовного процесса при расследовании преступлений экстремистской и террористической направленности: зарубежный опыт // Соотношение национального и международного права по противодействию национализму, фашизму и другим экстремистским преступлениям: материалы междунар. науч.-практич. конф., посвящ. выдающемуся российскому ученому Николаю Сергеевичу Алексееву (Москва, 30 окт. 2015 г.) / под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. С. 60–69.

Василий Васильевич презентовал отдельные положения своей уже готовой диссертации по киберэкстремизму[1].

Весть о его безвременном уходе застала меня в Нью-Йорке, где в штаб-квартире ООН с 29.01.2024 по 09.02.2024 проходила заключительная сессия Спецкомитета по разработке Конвенции ООН против киберпреступности (принята Генассамблеей ООН 24.12.2024)[2], «на полях» которой для продвижения российских подходов в Конвенцию состоялась также презентация нашей делегацией англоязычного издания коллективной монографии «Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы», в которой были использованы результаты исследований Василия Васильевича по проблематике цифровых следов преступлений[3] (впоследствии он ввел в научный оборот уточненный термин «(идеальные) закодированные информационные следы преступлений»[4]). Сам он всегда интересовался ходом работы над проектом Конвенции. Совсем

---

[1] Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 26–31.

[2] Полное «компромиссное» название договора – Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям от 24.12.2024 (далее также – Конвенция, Конвенция ООН, Конвенция 2024 г.).
Все приводимые в настоящей работе материалы, связанные с Конвенцией, опубликованы на официальном интернет-сайте Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях: URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (дата обращения: 15.03.2025).

[3] Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow: Publishing House “Gorodets”, 2024. 224 p.

[4] Бычков В.В. Теория и практика расследования преступлений экстремистской направленности...С. 74–75; Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом… С. 104–109, 153–154, 295.

незадолго до той командировки мы переговорили с ним по телефону и условились о встрече у него в Академии по моем возвращении, которой уже никогда не суждено было состояться.

Хочется добрым словом вспомнить здесь надежных соратников Василия Васильевича, которые содействовали реализации его творческих планов: его семью, А.М. Багмета, А.А. Бессонова, В.А. Прорвича, А.Ж. Саркисяна, С.В. Харченко и многих других друзей и коллег, сопровождавших этого замечательного человека на его жизненном пути.

В своем международном измерении досконально исследованный В.В. Бычковым феномен киберэкстремизма имеет сложную судьбу, что обусловлено дисбалансом ценностных установок в области прав человека на политической карте мира.

Российская Федерация участвует в большом количестве многосторонних универсальных секторальных[1], региональных[2] и двусторонних[3] межгосударственных договоров о международной правовой помощи в ее широком и узком значениях[4], межгосударственных, межправительственных и межведомственных[5]

---

[1] Конвенция ООН против транснациональной организованной преступности от 15.11.2000; Международная конвенция о борьбе с финансированием терроризма от 09.12.1999 и другие, в частности, антитеррористические конвенции.

[2] Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 07.10.2002; Европейская конвенция о выдаче от 13.12.1957 с Дополнительными протоколами; Европейская конвенция о взаимной правовой помощи по уголовным делам от 20.04.1959 с Дополнительными протоколами (применяются также по административно-деликтным производствам); Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16.05.2005 и другие конвенции.

[3] Например, Договор между Российской Федерацией и Республикой Польша о правовой помощи и правовых отношениях по гражданским и уголовным делам от 16.09.1996.

[4] См. подробнее о правовой помощи и правоохранительном содействии: Сотрудничество прокуратур в рамках Содружества Независимых Государств: учеб. пособие / авт. коллектив; под общ. ред. В.П. Зимина, науч. ред. А.А. Тимошенко; Ун-т прокуратуры Рос. Федерации. М., 2024. С. 86–96.

[5] Заключаемых Генеральной прокуратурой РФ, СК России, ФСБ России, МВД России, Минюстом России, Росфинмониторингом, Банком России, Роскомнадзором и ФТС России.

международных договоров и договоренностей о международном правоохранительном содействии, сотрудничестве подразделений финансовой разведки, в области банковского надзора и надзора в информационной сфере, применимых и применяемых к противодействию преступлениям и административным правонарушениям в сфере экстремизма в целом и киберэкстремизма в частности, в том числе отчасти к их предупреждению. УПК РФ и КоАП РФ предусматривают возможность испрашивания и оказания соответствующих видов правовой помощи также на основе принципа взаимности[1].

Однако здесь мы имеем дело с рядом серьезных препятствий и других проблем.

Первая из них состоит в том, что лишь весьма ограниченное число подобных международно-правовых актов содержат юридически обязательные нормы, посвященные правовой помощи и правоохранительному содействию в отношении преступлений и иных правонарушений именно в сфере экстремизма, единичные – в сфере киберэкстремизма, определенно выраженным образом называя их в качестве предмета сотрудничества сторон данного рода. На универсальном уровне таких международных договоров и иных

Так, Генеральной прокуратурой РФ во все заключаемые в настоящее время международные договоренности о сотрудничестве включаются вопросы противодействия экстремизму; также регулярно подписываются межведомственные договоренности с зарубежными визави, предусматривающие проведение совместных программных мероприятий по противодействию распространению экстремистской идеологии и использованию сети «Интернет» в экстремистских целях. Продолжается работа над проектом соглашения о сотрудничестве генеральных прокуратур государств – участников СНГ в противодействии терроризму и экстремизму, которое должно прийти на смену Соглашению о сотрудничестве генеральных прокуратур (прокуратур) государств – участников Содружества Независимых Государств в борьбе с терроризмом и иными проявлениями экстремизма от 25.05.2006.

[1] Принцип взаимности не учтен в Федеральном законе от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (ст. 17), обусловливающем наличием международного договора РФ сотрудничество в области борьбы с экстремизмом с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями, осуществляющими борьбу с экстремизмом. Подобная проблема присутствует и в Федеральном законе от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (п. 6 ст. 7, п. 3 ст. 14).

юридически обязывающих документов международного характера (резолюций Совета Безопасности ООН) сейчас, в отличие от антитеррористических конвенций и резолюций, нет и в обозримом будущем не предвидится, несмотря на имеющиеся резолюции как Генассамблеи, так и Совбеза ООН о других аспектах борьбы с экстремизмом[1].

Вторая проблема заключается в различном толковании содержания понятия экстремистской деятельности в национальных правовых системах государств, включая и те из них, что закрепили упомянутые обязательства между собой. Частный случай и отчетливое выражение данной проблемы – отсутствие механизма межгосударственного взаимного (автоматического) признания организаций экстремистскими на региональном, субрегиональном и двустороннем уровнях по типу листирования Совбезом ООН: механическая компиляция отдельных национальных перечней (списков) таких организаций[2] не переходит в новое, межгосударственное качество и не образует какой-либо значимой, юридически обязывающей синергии для сотрудничества.

В свою очередь, основные несовпадения в толковании касаются, во-первых, разных подходов к определению объема прав человека и гражданина в их взаимоотношениях как с такими же людьми, так и с органами и представителями публичной власти, внутри своей страны или за ее пределами; во-вторых, к защите международным правом интересов национальной безопасности государства.

Устоявшимся на глобальном уровне, относительно общепризнанным в мировом сообществе сейчас можно считать запрет экстремизма в форме насилия (физического, психологического), угроз насилием и подстрекательства к насилию (в чуть меньшей мере – к дискриминации, нетерпимости, розни, вражде)

---

[1] Антиэкстремистские инструменты и механизмы, имеющиеся на универсальном и региональном уровнях, освещены в работе: Мельшина К.Ю. Международно-правовые средства борьбы с экстремизмом: дис. … канд. юрид. наук. М., 2018. 268 с.

[2] Решение Комитета секретарей советов безопасности Организации Договора о коллективной безопасности от 08.06.2016 «О Перечне организаций, признанных террористическими и экстремистскими в государствах – членах Организации Договора о коллективной безопасности»; Списки организаций, признанных террористическими и экстремистскими в соответствии с законодательством государств – участников СНГ // АТЦ СНГ: [сайт]. URL: https://www.cisatc.org/1289/133/9133 (дата обращения: 15.03.2025).

в отношении определенных групп физических лиц, объединенных общими идентификационными признаками, и так называемого языка ненависти (включая новомодные концепции фундаментализма, онлайн-радикализации, геймификации экстремизма); бесспорной признается необходимость порицания и наказуемости расового, этнического, национального и религиозного экстремизма, в то время как подходы к проявлениям политической и социальной (сексистской, спортивной (в среде болельщиков) и др.) нетолерантности, отрицанию Холокоста, пропаганде нацизма – более нюансированные и не столь однозначные[1].

В то же время основы конституционного строя, территориальная целостность и другие существенные интересы государства в области его национальной безопасности пользуются значительно меньшей международно-правовой защитой от экстремистских посягательств, не исключая и насильственные, за действиями по их подрыву далеко не всегда признается преступный характер и, как следствие, статус объекта межгосударственного антикриминального сотрудничества. Таковая защита, как правило, является предметом взаимных обязательств государств-единомышленников, разделяющих взгляды на традиционные ценности государственного устройства, правопорядка и их охрану, на региональном, субрегиональном и двустороннем уровнях[2].

---

[1] См.: Международный пакт о гражданских и политических правах от 16.12.1966 (п. 2 ст. 20); Международная конвенция о ликвидации всех форм расовой дискриминации от 21.12.1965; принимаемые ежегодно по российской инициативе резолюции Генеральной Ассамблеи ООН «Борьба с героизацией нацизма, неонацизмом и другими видами практики, которые способствуют эскалации современных форм расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости»; OHCHR and freedom of expression vs incitement to hatred: the Rabat Plan of Action // Управление Верховного комиссара ООН по правам человека: [сайт]. URL: https://www.ohchr.org/en/freedom-of-expression (дата обращения: 15.03.2025); United Nations Strategy and Plan of Action on Hate Speech // ООН: [сайт]. URL: https://www.un.org/en/hate-speech/un-strategy-and-plan-of-action-on-hate-speech (дата обращения: 15.03.2025).

[2] См. об этом, например: Волеводз А.Г., Ализаде В.А. Международно-правовые подходы к противодействию экстремизму: материально-правовые и процессуальные аспекты // Международное уголовное право и международная юстиция. 2018. № 6. С. 7–11; Ульянов М.В. Использование банков данных субъектами противодействия экстремизму // Цифровые технологии в прокурорской деятельности: Сб. материалов конф. (Москва, 31 октября 2023 г.) / Под ред. Н.В. Субановой. М.: ИД «Городец», 2024. С. 223–229.

Так, наиболее развитая многоуровневая и многоаспектная договорно-правовая база антиэкстремистского сотрудничества, в том числе правовой помощи и полицейского содействия по уголовным и административно-деликтным производствам, сформирована в рамках ШОС[1], в меньшей степени – СНГ[2] и ОДКБ[3]; профильный

[1] Договор о долгосрочном добрососедстве, дружбе и сотрудничестве государств – членов Шанхайской организации сотрудничества от 16.08.2007 (ст. 8); Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15.06.2001; Конвенция Шанхайской организации сотрудничества по противодействию экстремизму от 09.06.2017; Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 (п. 5 Приложения 2); Соглашение о сотрудничестве между правительствами государств – членов Шанхайской организации сотрудничества в борьбе с преступностью от 11.06.2010 (ст. 1); Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве и взаимопомощи в таможенных делах от 02.11.2007 (ст. 5) («Таможенные службы в возможно короткие сроки передают по собственной инициативе или по запросу всю необходимую информацию о готовящихся или совершенных нарушениях таможенного законодательства государства одной из Сторон при перемещении литературы, аудио и видео материалов террористической и/или экстремистской направленности или имеющих признаки разжигания вражды и розни на межнациональной и/или межконфессиональной основе»).

[2] Соглашение об обмене информацией в рамках Содружества Независимых Государств в сфере борьбы с терроризмом и иными насильственными проявлениями экстремизма, а также их финансированием от 03.11.2017; Соглашение об обмене информацией в сфере борьбы с преступностью от 22.05.2009; не являющиеся юридически обязывающими Модельный закон «О противодействии экстремизму», принятый постановлением Межпарламентской Ассамблеи государств – участников СНГ от 14.05.2009 № 32-9, Рекомендации по совершенствованию законодательства государств – участников СНГ в сфере противодействия экстремизму, принятые постановлением Межпарламентской Ассамблеи государств – участников СНГ от 23.11.2012 № 38-16.

[3] См., например, Протокол о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере от 23.12.2014 (ст. 3); постановление Парламентской Ассамблеи Организации Договора о коллективной безопасности от 26.11.2015 № 8-3 «О проекте Рекомендаций по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере противодействия терроризму и экстремизму»; постановление Парламентской Ассамблеи Организации Договора о коллективной

двусторонний договор по рассматриваемой тематике Россией до настоящего времени заключен лишь с одним государством – Китаем[1].

Применительно к киберэкстремизму Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28.09.2018 в ст. 3 о криминализации закрепляет, что Стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых поименованные в этой статье деяния в сфере информационных технологий, если они совершены умышленно, в числе которых – «распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном *(национальным законодательством – прим. автора)* порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма».

С остальными же – тоже относительно немногими – странами юридически обязывающее взаимное противодействие именно экстремизму в его аналоговой и (или) цифровой ипостасях помещено не в специализированный, а в менее отчетливый общий договорно-правовой формат – в одном ряду перечисления с другими уголовно наказуемыми деяниями в межправительственных соглашениях о

безопасности от 19.12.2023 № 16-7.3 «О проекте модельного Руководства компетентных органов государств – членов ОДКБ в сфере оперативно-разыскного обеспечения коллективной безопасности» (предусматривает проведение в соответствии с национальным законодательством государств-членов и документами ОДКБ компетентными органами оперативно-разыскных мероприятий и действий в реальной и виртуальной (цифровой) средах, которые направлены в числе иного на противодействие экстремизму, терроризму, трансграничным преступлениям, в зоне ответственности ОДКБ путем использования специальных сил, средств и методов ОРД в условиях освоения новых ИКТ).

В рамках ШОС, СНГ и ОДКБ приняты и многие тематические документы «мягкого права» – политические совместные заявления, позиции, декларации, «дорожные карты» – стратегии, концепции и программы сотрудничества, планы действий; в СНГ и ОДКБ также модельные законы и другие акты рекомендательного характера, направленные на гармонизацию и сближение национальных законодательств государств-членов.

[1] Соглашение между Российской Федерацией и Китайской Народной Республикой о сотрудничестве в борьбе с терроризмом, сепаратизмом и экстремизмом от 27.09.2010.

сотрудничестве в борьбе с преступностью, в обеспечении международной информационной безопасности, в межведомственных договоренностях и некоторых других[1].

По линии Совета Европы специализированным договором о противодействии киберэкстремизму является Дополнительный протокол к Конвенции о киберпреступности, касающийся криминализации действий расистского и ксенофобского характера, совершенных посредством компьютерных систем от 28.01.2003 (Россия не участвует)[2].

Совокупность вышеупомянутых факторов в большинстве случаев приводит к отказу от межгосударственного антиэкстремистского взаимодействия по политизированным и правочеловеческим мотивам.

---

[1] См., например: Договор о дружественных отношениях и всеобъемлющем стратегическом партнерстве между Российской Федерацией и Монголией от 03.09.2019 (ст. 7); Соглашение между Правительством Российской Федерации и Правительством Республики Союз Мьянма о сотрудничестве в области обеспечения международной информационной безопасности от 05.12.2023 (ст. 2) («взаимодействие в правоохранительной сфере по предупреждению, выявлению, пресечению и расследованию правонарушений и преступлений, связанных с использованием информационно-коммуникационных технологий в террористических, экстремистских и иных преступных целях»); Соглашение между Правительством Российской Федерации и Правительством Чешской Республики о сотрудничестве в области борьбы с преступностью от 08.12.2011 (ст. 1) («Сотрудничество осуществляется прежде всего […] в борьбе с терроризмом и его финансированием; проявлениями экстремизма, расовой нетерпимости и ксенофобии; преступлениями в сфере информационных технологий»); Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством внутренних дел Республики Мозамбик от 22.08.2019 (ст. 2) («Стороны осуществляют взаимодействие в предупреждении, выявлении, пресечении и раскрытии преступлений, в том числе совершенных организованной группой или преступным сообществом (преступной организацией), прежде всего […] экстремистской деятельности, в том числе террористических актов, а также финансирования терроризма; преступлений в сфере информационных технологий»).

[2] На европейском пространстве работает Европейская комиссия по борьбе с расизмом и нетерпимостью; в числе иных принята Рекомендация Комитета министров Совета Европы государствам-членам CM/Rec(2022)16 от 20.05.2022 о борьбе с языком ненависти; в Европейском союзе действует также Рамочное решение Совета ЕС 2008/913/JHA от 28.11.2008 о борьбе с определенными формами и выражениями расизма и ксенофобии посредством уголовного права.

В этом отношении показательна, в частности, политика глобальной международной межправительственной организации уголовной полиции Интерпола (опирающаяся в том числе на заключения и решения Совета ООН по правам человека, прецедентную практику Европейского Суда по правам человека[1], в текущее время характеризующиеся антироссийской направленностью) по отказу в предоставлении его каналов для сотрудничества по многим категориям дел о политическом и социальном экстремизме, не подпадающим под вышеупомянутое исключение. Интерпол подвергает инкриминируемое деяние оценке на предмет преобладающих элементов *(predominance test)* – доминируют ли в нем признаки общеуголовного преступления либо же преступления против государственной власти: чаша весов с насилием и подстрекательством к нему, а также языком ненависти в отношении определенных групп частных физических лиц перевешивает в пользу допустимости сотрудничества, а чаша с насильственными актами и призывами к ним против институтов и органов государственной власти – в сторону отказа от него[2].

Против межгосударственного взаимодействия в области противодействия киберэкстремизму традиционно идут в ход и положения международных договоров об отказе в оказании правовой помощи по делам о так называемых политических преступлениях, преступлениях, связанных с политическими преступлениями, преступлениях, совершенных по политическим мотивам, и (или) по которым у запрашиваемого государства имеются основания полагать о наличии политических, социальных и других дискриминационных мотивов уголовного преследования или наказания либо возможности нанесения ущерба положению лица по этим причинам вследствие оказания запрошенной помощи.

---

[1] См., в частности: Factsheet – Hate speech. November 2023; Key theme – Article 10 Hate speech (Last updated: 29/02/2024); Key theme – Articles 8, 13 and 14 Protection against hate speech (Last updated: 31/08/2024) // Европейский Суд по правам человека: [сайт]. URL: https://www.echr.coe.int/ (дата обращения: 15.03.2025); Case Law by the European Court of Human Rights of Relevance for the Application of the European Conventions on International Co-Operation in Criminal Matters. Strasbourg, 29 Oct. 2024 [PC-OC/Documents2011/PC-OC (2011)21rev18].

[2] Repository of Practice: Application of Articles 2 and 3 of INTERPOL's Constitution in the context of the processing of data via INTERPOL's Information System. Third ed. Nov. 2024. Lyon: ICPO – INTERPOL, 2024. 108 p.

Очевидно, что стремящиеся к нулю шансы на успех имеют попытки получить заграничную помощь или содействие в расследовании актов государственного экстремизма и других международно-противоправных деяний одной страны против другой страны[1], в том числе в киберпространстве, равно как по делам о «фейках» и дискредитации в отношении Вооруженных Сил и иных органов государственной власти, уничтожении памятников и т.п., которые тоже исследовались В.В. Бычковым.

До сих пор странам не удалось и еще долго не удастся договориться об общепризнанном определении на универсальном уровне крайнего насильственного проявления экстремизма – терроризма, не говоря уже о самом экстремизме в целом[2] (в то же время емкие конвенционные дефиниции терроризма, экстремизма и смежных с ними понятий закреплены, например, в упоминавшихся выше юридически обязательных региональных правовых актах ШОС). Неолиберальные установки коллективного Запада во главе с США и его сателлитов из числа развивающихся стран по абсолютизации

---

[1] Литвишко П.А. О российских инициативах по противодействию противоправному сбору доказательств в киберпространстве представителями иностранных государств и международных органов // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 93–101.

[2] В документах ООН указывается следующее. «Определение «терроризма» и «насильственного *(иногда некорректно передаваемого в русском языке как «воинствующего» – прим. автора)* экстремизма» является прерогативой государств-членов и должно соответствовать их обязательствам по международному праву, в частности международному праву в области прав человека». «Термины «насильственный экстремизм» и «терроризм» зачастую используются ошибочно как взаимозаменяемые. В то время как терроризм является формой насильственного экстремизма и терроризм также часто идеологически мотивирован, концептуальная основа терроризма, которая отличает его от насильственного экстремизма, – это создание страха и террора в качестве средства достижения цели». «Насильственный экстремизм … может служить питательной средой для терроризма»; «насильственный экстремизм и нетерпимость мотивируют террористическую деятельность». См.: Preventing violent extremism through education: a guide for policy-makers. Paris: UNESCO, 2017. P. 18–20; Plan of Action to Prevent Violent Extremism // ООН: [сайт]. URL: https://www.un.org/counterterrorism/plan-of-action-to-prevent-violent-extremism (дата обращения: 15.03.2025).

свободы мнения и его выражения принципиально противостоят процессу универсальной криминализации этого зла.

Так, на запросы российских следственных органов по уголовным делам о преступлениях экстремистской направленности в сфере ИКТ, направляемые Генеральной прокуратурой РФ в США (где сосредоточены основные провайдеры услуг мессенджеров и социальных сетей), традиционно поступают отказы Министерства юстиции США в их исполнении со ссылкой на первую поправку к Конституции США о свободе слова.

Российским внешнеполитическим ведомством отмечается, что «Российская Федерация совместно с единомышленниками отстаивает незыблемость ключевых параметров международного контртеррористического и антиэкстремисткого сотрудничества. Аргументировано ведем линию на недопущение принудительного навязывания односторонних «стандартов и правил». В частности, речь идет о спорной западной концепции «противодействия насильственному экстремизму» (ПНЭ), которая необоснованно усиливает крен в пользу правозащитной и гендерной проблематики в антитерроре, открывает дополнительные возможности для вмешательства во внутренние дела государств. […] В последнее время США и их союзники активно продвигают на международных площадках инициативу борьбы с «расово и этнически мотивированным терроризмом/насильственным экстремизмом» (РЭМТ/РЭМНЭ). Ее главная опасность – намеренное упрощение или игнорирование реальных причин нынешнего всплеска распространения в мире ультраправых, националистических настроений, включая возрождение на Западе идеологии нацизма, искусственное выделение этого направления для манипулирования вокруг темы «внешнего иностранного влияния» в угоду борьбы с внутриполитическими противниками»[1].

Совсем неудивительно поэтому, что многие тщетные попытки нашей страны вместе с государствами-единомышленниками провести в Конвенцию ООН против киберпреступности положения о киберэкстремизме априори не были обречены на успех, равно как небольшие шансы на него будут иметь усилия восполнить подобные положения в приемлемом объеме в Дополнительном протоколе к

[1] Противодействие терроризму и экстремизму // МИД России: [сайт]. 2023. 18 января. URL: https://mid.ru/ru/foreign_policy/international_safety/crime/1848368/ (дата обращения: 15.03.2025).

данной Конвенции, который будет разрабатываться в ООН в ближайшие годы. В то же время интерес наших партнеров по ШОС, БРИКС к разработанному (изначально по инициативе Узбекистана) для продвижения в рамках этих объединений проекту «дублирующего» универсальную Конвенцию ООН многостороннего межрегионального договора (текущее рабочее название – «конвенция о противодействии использованию информационно-телекоммуникационных технологий для подготовки и совершения преступлений, в том числе террористической направленности»), включающего положения о киберэкстремизме, на сегодняшний день можно охарактеризовать как почти несуществующий. К слову, ту же участь в Конвенции ООН против киберпреступности разделил и терроризм; в качестве дополнительных мотивов оставления его «за бортом» документа оппонентами указывалось на наличие достаточного глобального договорно-правового режима по противодействию терроризму, представленного Международной конвенцией о борьбе с финансированием терроризма от 09.12.1999 и другими секторальными антитеррористическими конвенциями, применимыми и к ИКТ-сфере.

Уместно привести здесь положения о киберэкстремизме из официально внесенного нашей страной в названный Спецкомитет ООН российско-китайского проекта 2021 г. конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях, поскольку он был выработан и согласован всеми заинтересованными федеральными государственными органами:

«Статья 21. Преступления, связанные с экстремистской деятельностью

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству распространения материалов, содержащих призывы к совершению противоправных деяний по мотивам политической, идеологической, социальной, расовой, национальной или религиозной ненависти и вражды, пропаганды или оправдания таких деяний, либо обеспечения доступа к ним, совершенных с использованием ИКТ.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве

преступления или иного противоправного деяния согласно его внутреннему законодательству унижения лица или группы лиц по признакам расы, национальности, языка, происхождения, отношения к религии, совершенных с использованием ИКТ».

Смежные и оказавшиеся столь же «непроходными» составы преступлений экстремистской направленности были закреплены в ст. 19 (подстрекательство к подрывной или вооруженной деятельности), 20 (преступления, связанные с террористической деятельностью) и 24 (реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности).

По нашим отечественным меркам это была довольно скромная запросная позиция, не содержавшая, конечно же, составы экстремистских посягательств на госбезопасность, не сопоставимая по своему охвату с перечнем преступлений экстремистской направленности в примечании 2 к ст. 282^1 УК РФ, а тем более видов экстремистской деятельности (экстремизма) в ст. 1 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности».

При этом речь идет о материально-правовой норме, которая предусматривала бы криминализацию, признание Конвенцией киберэкстремизма в качестве уголовно наказуемого деяния и подлежала бы имплементации в национальном законодательстве всех государств-участников в виде криминализации и пенализации деяния. Очевидно, что государства, традиционно склонные рассматривать в целом экстремизм в качестве преступного деяния, в большинстве случаев уже закрепили соответствующие положения в своих уголовных законах (в виде самостоятельных статей либо квалифицирующих «ИКТ-признаков»), а те, что этого делать принципиально не желают, попросту не станут добровольно принимать на себя такое обязательство по международному договору, становиться его участником.

Однако то, что норма о криминализации киберэкстремизма не вошла в Конвенцию 2024 г., вовсе не означает, что ее государства-участники, желающие этого, не смогут осуществлять двустороннее сотрудничество друг с другом на основе ее процессуально-правовых норм, без ущерба для вредоносности внедренных в нее коллективным Западом и беспрецедентных для антикриминального договора «правочеловеческих закладок» (прежде всего, это касается самого неконсенсусного п. 2 ст. 6, согласно которому «[ничто в настоящей

Конвенции не толкуется как допускающее подавление прав человека или основных свобод, включая права, касающиеся свободы выражения, совести, мнений, религии или убеждений, мирных собраний и объединений, в соответствии с применимыми нормами международного права прав человека»)[1].

Дело в том, что обязательства сторон Конвенции 2024 г. по международному сотрудничеству в обмене электронными доказательствами и в рамках сети 24/7 действуют, помимо установленных ею составов преступлений (среди которых киберэкстремизма нет), также в отношении неограниченного круга других «серьезных преступлений», как они определены в национальном праве сторон, среди которых, это очевидно, может быть и киберэкстремизм. Кроме того, Конвенция допускает исполнение запросов по делам о деяниях, которые не отвечают требованию двойной криминализации, об административных правонарушениях, на правах исключения из правила об отказе – по свободному усмотрению запрашиваемой стороны, по аналогии с Конвенцией ООН против транснациональной организованной преступности 2000 г. (Палермской конвенцией) и некоторыми другими конвенциями. Наконец, стоит отметить и наличие в Конвенции нормы о предоставлении взаимной правовой помощи по делам об ответственности юридических лиц, которая исследована В.В. Бычковым в основном в контексте иностранных агентов и нежелательных организаций, причастных к деятельности в сфере киберэкстремизма.

Вместе с тем охват и такого международного сотрудничества заужен путем установления Конвенцией его основных форм исключительно в отношении преступлений, признанных таковыми в соответствии с ней (установленных в главе о криминализации), в частности, это касается экстрадиции, передачи на время содержащегося под стражей лица, передачи уголовного производства, совместных расследований, принятия любых обеспечительных и конфискационных мер в отношении активов и даже блока правоохранительного содействия (ст. 47). В Конвенцию не вошла и востребованная для противодействия киберэкстремизму

[1] См. подробнее об этом и о Конвенции в целом: Литвишко П. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. 2024. № 11. С. 4–27.

классическая норма о специальных методах расследования (негласных оперативно-разыскных мероприятиях, в данном случае в киберпространстве), имеющаяся в Палермской конвенции и других универсальных инструментах.

Стоит упомянуть, что обходить условие двойной криминализации и иные препятствия для международной правовой помощи по делам о киберэкстремизме возможно в целом ряде случаев за счет эффективного применения консульской правовой помощи по уголовным делам, без обращения к иностранным органам, в особенности «недружественных» государств[1].

Генеральная прокуратура РФ, как главный центральный орган России в сфере правовой помощи и правовых отношений по уголовным делам, всегда обращает внимание партнеров, что по большинству современных международных договоров и имплементационному законодательству к ним для оказания международной правовой помощи в ее узком смысле – выполнения отдельных следственных и иных процессуальных действий, не имеющих принудительного, интрузивного характера, не вторгающихся в основные права и свободы человека и гражданина, – соблюдения требования двойной преступности деяния не требуется.

Это не относится к некоторым другим видам международной правовой помощи в ее широком смысле, в частности, к экстрадиции, принятия уголовного преследования, в рамках которых деяние должно являться уголовно наказуемым как в запрашивающем, так и запрашиваемом государстве, а в случае киберэкстремизма, обусловленного принадлежностью к экстремистской организации, таковая должна значиться в числе «листированных» в установленном порядке Советом Безопасности ООН и (или) российскими судами (двойная криминализация *in concreto vs. in abstracto*).

---

[1] Уголовный процесс России и стран Европы: сравнительно-правовое исследование: монография / под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2023. С. 174–205; Консульская правовая помощь: Информация о процессуальных действиях, которые могут выполняться консульскими должностными лицами Российской Федерации на основании запросов компетентных органов Российской Федерации о правовой помощи по уголовным, гражданским, административным делам, делам об административных правонарушениях // Генеральная прокуратура РФ: [сайт]. URL: https://epp.genproc.gov.ru/web/gprf/activity/international-cooperation/help (дата обращения: 15.03.2025).

Кроме того, в отличие от расового и подобных ему видов экстремизма против частных лиц, объекты и предметы составов экстремизма против государственной власти можно считать специальными, то есть соответствующая уголовно-правовая охрана нацелена на основы конституционного строя, территориальную целостность и национальную безопасность исключительно государства, чей уголовный закон запрещает эти деяния; в российском законе это соответственно конституционный строй по Конституции России, территория и безопасность России, а не какого-либо другого государства. Это может препятствовать, в частности, применению положений ст. 12 УК РФ об экстратерриториальном действии российского уголовного закона; ст. 458–459 УПК РФ о передаче за рубеж и принятии из-за рубежа уголовного преследования; гл. 55 УПК РФ о принятии и передаче лица, осужденного к лишению свободы, для отбывания наказания в государстве, гражданином которого оно является, принятии и передаче исполнения наказания, не связанного с лишением свободы, а также применения условного осуждения или отсрочки отбывания (исполнения) наказания государством (в государство), гражданином которого является осужденный; гл. 55^1 о признании и принудительном исполнении приговора, постановления суда иностранного государства в части конфискации находящихся на территории Российской Федерации доходов, полученных преступным путем. Те же ограничения могут действовать зеркально – со стороны иностранного государства, у которого Россией запрошена правовая помощь этих видов.

Как показано, проблема международного противодействия киберэкстремизму имеет многогранный и даже в очень долгосрочной перспективе трудноразрешимый характер. Поэтому лишь закономерно то, что с присущим ему стремлением браться именно за новые и сложные вызовы современности, не ища проторенных путей, своими трудами В.В. Бычков внес существенный вклад в эту продолжающуюся дискуссию планетарных масштаба и значимости. Нет никаких сомнений в том, что научная мысль и дело Василия Васильевича будут всегда жить и приумножаться будущими поколениями юристов.

Список источников

1. Бычков В.В. К вопросу об актуальности научных исследований проблем противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 26–31.

2. Бычков В.В. Особенности производства допросов при расследовании преступлений экстремистской направленности // Соотношение национального и международного права по противодействию национализму, фашизму и другим экстремистским преступлениям: материалы междунар. науч.-практич. конф., посвящ. выдающемуся российскому ученому Николаю Сергеевичу Алексееву (Москва, 30 окт. 2015 г.) / под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. С. 60–64.

3. Бычков В.В. Противодействие преступлениям экстремистской направленности. М.: Изд-во «Юрлитинформ», 2013. 256 с.

4. Бычков В.В. Теория и практика расследования преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей: дис. … д-ра юрид. наук. М., 2023. 722 с. (неопубликованная рукопись).

5. Бычков В.В., Литвишко П.А. Идентификация по татуировкам участников уголовного процесса при расследовании преступлений экстремистской и террористической направленности: зарубежный опыт // Соотношение национального и международного права по противодействию национализму, фашизму и другим экстремистским преступлениям: материалы междунар. науч.-практич. конф., посвящ. выдающемуся российскому ученому Николаю Сергеевичу Алексееву (Москва, 30 окт. 2015 г.) / под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. С. 65–69.

6. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д.ю.н., д.т.н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. 572 с.

7. Волеводз А.Г., Ализаде В.А. Международно-правовые подходы к противодействию экстремизму: материально-правовые и

процессуальные аспекты // Международное уголовное право и международная юстиция. 2018. № 6. С. 7–11.

8. Литвишко П. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. 2024. № 11. С. 4–27.

9. Литвишко П.А. О российских инициативах по противодействию противоправному сбору доказательств в киберпространстве представителями иностранных государств и международных органов // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 93–101.

10. Мельшина К.Ю. Международно-правовые средства борьбы с экстремизмом: дис. … канд. юрид. наук. М., 2018. 268 с.

11. Прорвич В.А. Научные и организационные основы государственной программы борьбы с киберэкстремизмом: творческое наследие Василия Васильевича Бычкова // Расследование преступлений: проблемы и пути их решения. 2024. № 1. С. 187–198.

12. Сотрудничество прокуратур в рамках Содружества Независимых Государств: учеб. пособие / авт. коллектив; под общ. ред. В.П. Зимина, науч. ред. А.А. Тимошенко; Ун-т прокуратуры Рос. Федерации. М., 2024. 100 с.

13. Уголовный процесс России и стран Европы: сравнительно-правовое исследование: монография / под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2023. 280 с.

14. Ульянов М.В. Использование банков данных субъектами противодействия экстремизму // Цифровые технологии в прокурорской деятельности: Сб. материалов конф. (Москва, 31 октября 2023 г.) / Под ред. Н.В. Субановой. М.: ИД «Городец», 2024. С. 223–229.

15. Case Law by the European Court of Human Rights of Relevance for the Application of the European Conventions on International Co-Operation in Criminal Matters. Strasbourg, 29 Oct. 2024. [PC OC/Documents2011/PC-OC (2011)21rev18].

16. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow: Publishing House “Gorodets”, 2024. 224 p.

17. Factsheet – Hate speech. November 2023; Key theme – Article 10 Hate speech (Last updated: 29/02/2024); Key theme – Articles 8, 13 and 14 Protection against hate speech (Last updated: 31/08/2024) // Европейский Суд по правам человека: [сайт].
18. OHCHR and freedom of expression vs incitement to hatred: the Rabat Plan of Action // Управление Верховного комиссара ООН по правам человека: [сайт].
19. Plan of Action to Prevent Violent Extremism // ООН: [сайт].
20. Preventing violent extremism through education: a guide for policy-makers. Paris: UNESCO, 2017. 75 p.
21. Repository of Practice: Application of Articles 2 and 3 of INTERPOL's Constitution in the context of the processing of data via INTERPOL's Information System. Third ed. Nov. 2024. Lyon: ICPO – INTERPOL, 2024. 108 p.
22. United Nations Strategy and Plan of Action on Hate Speech // ООН: [сайт].

К. И. Озеров[1], **И.Н. Озеров**[2]
[1]Межрегиональный открытый социальный институт
[2]Московская академия Следственного комитета
имени А.Я. Сухарева

Противодействие кибersталкингу как форме киберэкстремизма

Аннотация. Сегодняшняя информационная среда требует реагирования и ответа на главный вопрос как обеспечить безопасность общества и гражданина. Это обусловливает необходимость выработку механизма защиты людей и их социальных групп от различных форм, видов угроз и посягательств. Трансформация в цифровом обществе обуславливает сохранность адекватного механизма межличностных взаимоотношений, которое невозможно без обеспечения цифровой гигиены и соблюдения высоких цифровой морали и правосознания. Кибersталкинг как новое явление, выражается в использовании Интернета для преследования или домогательств человека, группы людей или организации, посредством поисковых сервисов, на онлайн форумах, в чатах и через социальные сети. В данной статье мы затрагиваем существующие проблемы, возникающие при современном цифровом пространстве,

где возможны новые формы агрессии, давления и противоправного поведения. Киберэкстремизм, представляющий собой проявление насильственной идеологии в сети, может быть зарожден на этапе кибersталкинга, как формы психологического и поведенческого насилия в интернете, часто не подпадающее под прямую уголовную квалификацию.

В настоящей статье рассматриваются теоретико-правовые аспекты кибersталкинга и киберэкстремизма, анализируются их сущностные характеристики, цели, формы проявления и возможности уголовно-правовой квалификации. Делается акцент на необходимости нормативного закрепления критериев цифрового насилия и совершенствования законодательной базы.

Данная статья предлагает рассмотреть кибersталкинг как предиктор деструктивного поведения в сети, сопоставить его с чертами киберэкстремистской деятельности и предложить модели реагирования в условиях пробелов в законодательстве.

Ключевые слова: киберэкстремизм, кибersталкинг, цифровой абьюз, цифровая гигиена, цифровая санитария.

Расширение цифровой среды открыло новые возможности как для конструктивной коммуникации, так и для трансформации форм насилия и давления. Одним из наиболее тревожных явлений является кибersталкинг — навязчивое и повторяющееся цифровое преследование. Хотя он традиционно рассматривается как частное, межличностное нарушение, современные тенденции свидетельствуют: в определённых условиях кибersталкинг может перерастать в более широкую, социально опасную активность, близкую по характеру к киберэкстремизму.

Кибersталкинг — это использование Интернета для преследования или домогательств человека, группы людей или организации.[1] Кибersталкинг охватывает комплекс действий, совершаемых с помощью интернета и цифровых технологий с целью установить контроль, причинить дискомфорт, унизить или запугать другого человека. По мнению Бычкова В.В., кибersталкинг как форму

[1] Cyberstalking – definition of cyberstalking in English from the Oxford dictionary. URL: oxforddictionaries.com. (Дата обращения: 22 марта 2024 г.).

киберэкстремизма следует рассматривать как "информационно-психологическую агрессию с элементами воздействия на идентичность жертвы, нарушающую её цифровую автономию"[1], совершаемых с помощью интернета и цифровых технологий с целью установить контроль, причинить дискомфорт, унизить или запугать другого человека.

Кибersталкеры ищут своих жертв посредством поисковых сервисов, на онлайн форумах, в чатах и через социальные сети. Они могут преследовать жертву ради удовлетворения своих одержимостей или любопытства.

Лерой МакФэрлэйн и Пол Босич в своей работе выделили четыре типа кибersталкеров: мстительные кибersталкеры, чьи атаки отличаются свирепостью своих атак; сквозные кибersталкеры, чьей задачей является раздражить жертву; интимные сталкеры, которые пытаются завести отношения с жертвой и начинают вести себя агрессивно, если отвергнуты; коллективные кибersталкеры, которые объединяются вокруг мотива.[2]

Мотивационная база разнообразна: от личной обиды и ревности до желания демонстративного подавления или мести. Кибersталкинг всё чаще используется не только для эмоционального давления, но и как способ длительного сетевого манипулирования с элементами идеологического заражения – в случаях, когда объектом становятся гражданские активисты, журналисты или религиозные меньшинства: от личной обиды и ревности до желания демонстративного подавления или мести.

Как нам представляется, вследствие разнообразия мотиваций и способов воздействия, кибersталкеры, чьи действия имеют признаки экстремистской направленности, могут быть классифицированы по следующим типам (см. *таблицу*).

---

[1] Бычков, В. В. Киберэкстремизм: понятие, квалификация, расследование / В. В. Бычков, В. А. Прорвич. Москва : Московская академия Следственного комитета Российской Федерации, 2023. 330 с. С. 43–44.

[2] McFarlane, Leroy & Bocij, Paul An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday,* 2003-08-04, vol. 8, iss. 9.

Типы кибersталкеров

Тип кибersталкера	*Характеристика*	*Примеры из практики*
1. Идеологически мотивированный	Преследует жертву на основе её взглядов, убеждений, принадлежности к группе	В 2022 г. в Татарстане возбуждено дело против студента, систематически угрожавшего преподавателю за проукраинскую позицию в сети
2. Политический активист-радикал	Использует сталкинг как элемент давления на оппонентов или чиновников	Группа лиц из закрытого Telegram-канала в Москве организовала координированную травлю кандидата в депутаты — с публикацией личных данных
3. Экс-участник группировки	Преследует бывших соратников или оппонентов в рамках «идеологической мести»	Бывший участник неонацистской группы мстил информатору, раскрывшему деятельность ячейки
4. Информационный волонтёр»	Считает себя борцом с «иными» — религиозными, сексуальными, этническими меньшинствами; действует «от лица народа»	В Красноярском крае осуждён гражданин, публиковавший угрозы в адрес раввина, считая, что тот «разлагает традиции»
5. Анонимный сетевой координатор	Руководит группами в мессенджерах, организует массовые нападения через ботов и фейки	В 2023 году в Свердловской области была заблокирована группа, где администратор организовывал «наезды» на журналистов либеральных изданий
6. Сетевой мститель/инсайдер	Имеет доступ к приватной информации, использует её в целях давления, дискредитации	Следственный комитет Пермского края завёл дело против ИТ-администратора школы, угрожавшего ученикам, поддерживавшим определенное неформальное движение

Новые веяния времени требуют понимания о происходящих иных формациях в обществе, при которых должны быть сохранены адекватные механизмы межличностных взаимоотношений на основе соблюдения высокой нравственности, морали и этики. Вместе с тем, требуется изучение формирования правил поведения в аспекте информатизации особенно молодого поколения, соблюдение которых было бы направлено на повышение безопасности личности. Возникающая множественность субъектов, стремящихся доминировать в освоении и внедрении цифровых технологий, приводит к ускорению перемен в жизни общества. Это провоцирует ситуацию, когда привычные для общества модели поведения и институты, определяющие его развитие на протяжении длительного периода времени, утрачивают свою актуальность намного быстрее, оказываясь не способными своевременно принимать необходимые решения и шаги для предупреждения рисков.

Информационно-телекоммуникационные технологии позволяют группам анонимных людей самоорганизовываться для того, чтобы искать жертв для цифровых атак. Это может включать в себя отправку вредоносных сообщений по электронной почте. А также нередко кибersталкеры манипулируют поисковыми системами, чтобы сделать контент, более популярным в Сети. Такого рода действия часто вынуждают жертв использовать псевдоним или полностью уходить в офлайн.[1]

В зависимости от контекста кибersталкинг может включать: наблюдение за активностью жертвы через соцсети; навязчивую коммуникацию, включая угрозы, манипуляции, оскорбления; дискредитацию через распространение ложной или конфиденциальной информации; создание виртуальных клонов с целью подрыва репутации жертвы; вовлечение третьих лиц в травлю (так называемый «координированный сталкинг»).

Анализ судебных и следственных материалов позволяет зафиксировать случаи, в которых кибersталкинг носит не индивидуальный, а групповой, идеологически окрашенный характер. В частности: преследование лиц по признаку политической или гражданской позиции; координация действий через закрытые каналы с целью давления на представителей медиа, НКО, профсоюзов;

[1] Озеров И.Н. Кибersталкинг – «цифровой абьюз» или преступление? / И.Н. Озеров, Э.С. Сарыгина, К.И. Озеров // Международный вестник криминалистики. 2024. № 2(90). С. 24–34.

вовлечение в сетевые кампании с признаками публичного разжигания ненависти или вражды.

В таких случаях целенаправленный кибersталкинг трансформируется в инструмент киберэкстремизма. Его главная особенность – системность, публичность и наличие идеологического подтекста.

Сегодня кибersталкинг не выделен в самостоятельный состав ни в уголовном, ни в административном законодательстве. Это приводит к ряду проблем: квалификация по статьям 119, 137, 128.1 УК РФ требует доказательств угрозы или ущерба, что трудно установить в цифровом пространстве; отсутствие правового определения сталкинга делает невозможной типизацию правонарушений и сбор аналитики; кибersталкинг, переходящий в идеологическое давление, часто ускользает от уголовной ответственности из-за отсутствия прямых призывов к насилию.

Пока граждане и социальные группы людей накапливают негативный опыт по соблюдению цифровой гигиены, дают советы по санитарии в сфере цифровой реальности, которые не имеют отношение к общепризнанным правилам, деструктивное влияние анонимных пользователей влияет на них, посредством сталкерства в сети. Кибersталкеры пытаются нанести вред компьютеру жертвы, посылая ему вирусы. Сталкинг – это продолжительный процесс, состоящий из серии действий, каждая из которых может быть легальной по отдельности.

В целях повышения эффективности противодействия данному явлению крайне необходимы меры по правовому и организационному регулированию, а именно: признание кибersталкинга как основания для начала оперативной проверки при наличии идеологической или публичной направленности; введение отдельной нормы в УК РФ — «цифровое преследование» с квалифицирующими признаками (идеологическая мотивация, системность, воздействие на общественную безопасность); разработка административной статьи в КоАП РФ для случаев без выраженного уголовного ущерба (аналог нормы о домашнем насилии); создание специализированных подразделений при УВД и СК РФ по делам цифрового преследования; расширение полномочий Роскомнадзора и экспертных центров по мониторингу деструктивного онлайн-преследования.

Противодействие кибersталкингу требует сочетания правовых, технических и профилактических мер. Среди наиболее актуальных направлений можно выделить: разработку отдельной нормы в УК РФ о цифровом преследовании с указанием форм, мотивов и квалифицирующих признаков; внесение дополнений в КоАП РФ об ответственности за повторяющееся нежелательное цифровое воздействие; уточнение признаков угроз и преследования в цифровом контексте через постановления Пленума ВС РФ.

Кибersталкинг, хотя и воспринимается как личностное насилие, в ряде случаев может выступать звеном в цепочке радикализации и экстремизации, особенно при наличии публичного компонента и идеологического окраса. Его игнорирование на ранних стадиях может привести к резонансным последствиям. Разработка механизмов ранней квалификации, фиксации цифровых следов и институционального реагирования позволит не только защитить жертв, но и предупредить использование кибersталкинга как «мягкой» формы цифрового экстремизма. Для чего необходимо расширение полномочий подразделений МВД по киберпреступности в части доступа к технической информации при угрозах сталкинга; ведение наблюдения и фиксации цифровой активности подозреваемого (мониторинг переписок, IP-логов, активности в сетях); установление личности киберпреследователя с использованием данных цифровых платформ.

Кроме того для повышения эффективности расследования уголовных дел данной категории значительное внимание уделяется назначению компьютерно-технических и психолого-лингвистических экспертиз для анализа цифровых сообщений, переписок, публикаций и установления признаков преследования; обеспечения доступа к облачным хранилищам, аккаунтам и удалённым серверам, где могут находиться материалы, подтверждающие навязчивое поведение; получению судебных санкций на изъятие цифровых носителей, а также обеспечение их надлежащей фиксации (хэш-суммы, протоколы); допросу потерпевших и свидетелей с применением психологических методик для выявления элементов давления, страха и нарушения личной свободы; взаимодействию с подразделениями МВД и Роскомнадзора для проведения оперативных мероприятий по установлению IP-адресов, геолокации, регистрации учётных записей.

Не обойти стороной и обеспечить среди мер противодействия кибersталкингу разработку стандартов фиксации цифрового вреда (скриншоты, видеофиксация, экспертные заключения); поддержку потерпевших при обращении в суд, включая использование электронных доказательств; внедрение специальных процедур защиты жертв цифрового преследования (аналог программ защиты свидетелей).

Кроме того, весьма эффективными могут быть платформенные и технологические меры: введение обязательств для цифровых платформ по реагированию на жалобы о кибersталкинге в срок не более 24–48 часов; технологические решения: фильтрация контента, автоматическая блокировка повторных агрессоров, чёрные списки по IP; создание каналов обратной связи с правоохранительными органами для быстрой передачи информации.

Не стоит забывать и о профилактике, в контексте цифрового образования, а именно включении в школьные и университетские программы тематики цифрового этикета, распознавания агрессии, способов самообороны в сети; информационных кампаниях по недопущению участия в цифровой травле; психологической помощь лицам, пострадавшим от цифрового насилия, и предотвращение вторичной виктимизации.

Подводя итог, приходим к выводу, что современные угрозы в цифровой среде требуют переосмысления традиционного подхода к правонарушениям. Кибersталкинг, хотя и воспринимается как личностное насилие, в ряде случаев может выступать звеном в цепочке радикализации и экстремизации, особенно при наличии публичного компонента и идеологического окраса. Его игнорирование на ранних стадиях может привести к резонансным последствиям.

Разработка механизмов ранней квалификации, фиксации цифровых следов и институционального реагирования позволит не только защитить жертв, но и предупредить использование кибersталкинга как «мягкой» формы цифрового экстремизма.

Список источников

1. McFarlane, Leroy & Bocij, Paul An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday*, 2003-08-04, vol. 8, iss. 9.

2. Бычков В.В. Противодействие киберэкстремизму: правовые и организационные аспекты // Информационное право. 2022. № 4. С. 22–27

3. Бычков, В.В. Киберэкстремизм: понятие, квалификация, расследование / В.В. Бычков, В.А. Прорвич. М.: Московская академия СК России, 2023. 330 с.

4. Васильев А.Л. Киберэкстремизм как феномен цифровой среды // Право и цифровизация. 2023. № 1. С. 48–55.

5. Озеров И.Н. Кибersталкинг – «цифровой абьюз» или преступление? / И.Н. Озеров, Э.С. Сарыгина, К.И. Озеров // Международный вестник криминалистики. 2024. № 2(90). С. 24–34.

6. Озеров И.Н., Сарыгина Э.С. О цифровой санитарии современного общества // Проблемы правоохранительной деятельности. 2022. № 1. С. 6–10.

7. Прорвич В.А. Особенности уголовно-правовой защиты субъектов цифровых прав в условиях перехода к информационному обществу // Александр Яковлевич Сухарев: служение Отечеству в праве и науке: Материалы Всероссийской научно-практической конференции, Москва, 13 октября 2023 года. Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. С. 102–111.

8. Сарыгина Э.С., Озеров И.Н. Цифровая гигиена и цифровая санитария в аспекте информационной безопасности молодого поколения // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: Материалы международной научно-практической конференции, Москва, 2–3 декабря 2021 г. Москва: Московская академия Следственного комитета, 2022. С. 83–88.

Н.В. Османова
Московская академия Следственного комитета
имени А.Я. Сухарева

К вопросу об определении форм уголовного преследования на досудебной стадии уголовного производства

Аннотация. Анализируются формы уголовного преследования, их сходства и различия, соотношение институтов предъявления обвинения и уведомления о подозрении. В статье предлагается оптимизация форм предварительного расследования посредством предоставления равных гарантий таким участникам уголовного судопроизводства, как подозреваемый и обвиняемый. Делается вывод, представляющий интерес для дальнейших научных разработок и получения новых знаний о форме досудебного уголовного производства.

Ключевые слова: судебная реформа, уголовное преследование, предварительное следствие, дознание, упрощенное производство, подозрение, обвинение, субъект уголовного преследования.

В поисках оптимальной модели осуществления уголовного преследования в более короткие сроки (по сравнению с действующим законодательством) законодателем предпринимались неоднократные попытки внедрения упрощенных процедур уголовного преследования на досудебной стадии уголовного судопроизводства.

В различные этапы развития уголовно-процессуального законодательства к таким процедурам относились дознание, протокольная форма расследования, дознание в отношении конкретного лица, дознание по делам, по которым лицо не установлено, с последующей передачей уголовного дела в следственный орган.

При создании дознания как формы расследования разработчиками УПК РФ отмечалось, что при осуществлении расследования в предлагаемой упрощенной форме не будет требоваться проведения

«сверхсложных экспертиз» или «сверхдоказательств»[1], а само расследование не займет много времени. Без сомнения, одной из задач повышения эффективности уголовного судопроизводства является его оптимизация посредством сокращения срока между началом производства по уголовному делу и его окончанием. Процессуальные сроки всегда имели важное значение для уголовного судопроизводства, а также для обеспечения защиты участников процесса от неоправданно длительного производства по делу. В УПК РСФСР (ст. 2) в качестве одной из задач уголовного судопроизводства была закреплена быстрота раскрытия преступлений.

К сожалению, включение в ч. 2 ст. 223 УПК РФ (в ред. Федерального закона от 04.07.2003 № 92-ФЗ) положения о том, что расследование в форме дознания проводится по уголовным делам, возбуждаемым в отношении конкретных лиц, на практике привело к серьезной правовой коллизии. Требования указанной нормы, установившие предельный срок дознания 30 суток, привели к значительному увеличению количества уголовных дел, передаваемых из органов дознания в органы предварительного следствия.

При этом производство по уголовному делу в форме дознания как в отношении конкретного, так и в отношении неустановленного лица, практически ничем не отличались друг от друга, на что обращалось внимание в ходе заседания Межведомственной рабочей группы при Комитете по гражданскому, уголовному, арбитражному и процессуальному законодательству (17 февраля 2006 г.). Так, разница между дознанием и предварительным следствием, по мнению членов рабочей группы, заключается (по состоянию на февраль 2006 г.) в сроках и порядке окончания расследования[2], что является недостаточным. Следует согласиться с позицией авторов, согласно которой между предварительным следствием и дознанием «нет и не может быть глубоких институциональных или принципиальных различий. Они фактически совпадают по целям, задачам,

---

[1] Стенограмма конференции: «Уголовно-процессуальный кодекс Российской Федерации и проблемы правоприменительной практики» (26 февраля 2002 г.). Ярославль. 2002. С. 71.

[2] Стенограмма заседания Межведомственной рабочей группы при Комитете по гражданскому, уголовному, арбитражному и процессуальному законодательству (17 февраля 2006 г.). Москва. 2006. С. 13.

процессуальным средствам (круг следственных действий), месту в структуре уголовного процесса и т.д.»[1].

Следует отметить, что действительная оптимизация уголовного преследования возможна только в случае изменения отечественной доказательственной теории, ориентации ее на установление материальной (объективной) истины, концептуальные положения которой нашли свое отражение в трудах М.С. Строговича[2].

Анализ проводимой в России судебной реформы, упрощенных механизмов уголовного судопроизводства позволяет утверждать об одновременном усложнении существующих форм наряду с появлением наиболее простых. Качественными отличиями обладает, по нашему мнению, только дознание в сокращенной форме, ставшее закономерным последствием усложнения дознания и результатом поиска новой упрощенной формы производства по уголовному делу.

Одним из ключевых различий форм предварительного расследования является производство расследование следователем или дознавателем. Обратим внимание на п. 7 ч. 3 ст. 151 УПК РФ, согласно положениям которого и предварительное следствие, и дознание могут осуществляться следователем СК России. При этом порядок избрания мер принуждения зависит не от формы расследования, а от субъекта расследования – следователь СК России при избрании меры пресечения в виде заключения под стражу в ходе осуществлении дознания получает, как и при производстве предварительного следствия, согласие руководителя следственного органа, а не прокурора. Началом производства по уголовному делу независимо от формы предварительного расследования является принятие решения о возбуждении уголовного дела: проверка сообщения о преступлении, поводы и основания, а также сама процедура возбуждения уголовного дела, в том числе по делам частного обвинения (ч. 4 ст. 20 УПК РФ указывает именно на субъекта, осуществляющего расследование – следователя, а не на форму предварительного расследования), не имеет различий. В ходе производства следственных действий составляются одинаковые документы, порядок их осуществления, время производства и пр. – не зависят от формы производства. Согласование ходатайства

[1] Курс уголовного процесса / Под ред. Л.В. Головко. 2-е изд., испр. М., 2017. С. 651.

[2] Строгович М.С. Учение о материальной истине в уголовном процессе. М, 1947. 276 с.

о производстве следственного действия, затрагивающего конституционные права граждан (обыск в жилище) также обусловлено не формой предварительного расследования, а принадлежностью субъекта уголовного преследования к следственному органу или органу дознания.

В настоящее время вполне очевидно снижение значения такого критерия различия как порядок придания лицу статуса обвиняемого. Переход подозреваемого в новый статус после предъявления обвинения как в ходе предварительного следствия, так и при производстве дознания обусловлен достаточностью доказательств (ч. 1 ст. 171 УПК РФ) – относительной и весьма субъективной категорией. Институт уведомления лица о существующем в отношении него подозрении в совершении преступления, введенный Федеральным законом от 06 июня 2007 г. № 90-ФЗ, хоть и характерен только для дознания, в случае и при наличии волеизъявления законодателя, на наш взгляд, может быть распространен на расследование, осуществляемое в форме предварительного следствия.

Указанные выше различия, являются обязательными для соблюдения при производстве в той или иной форме, однако по своему содержанию не имеют существенных различий.

Полагаем, что ни уведомление о подозрении, ни привлечение лица в качестве обвиняемого не могут заменить друг друга при производстве предварительного расследования в различных формах. С позиции предоставления дополнительных гарантий участникам уголовного судопроизводства следует либо окончательно усложнить производство и сделать оба эти процессуальных института обязательными для дознания и предварительного следствия, либо отказаться от одного от них (при производстве предварительного расследования), упростив тем самым уголовно-процессуальные механизмы.

Вынесение постановления о привлечении лица в качестве обвиняемого, уведомление о подозрении формируют процессуальный статус лица, в отношении которого осуществляется уголовное преследование, определяя начало участия в уголовном деле защитника. Однако этот момент может быть по усмотрению следователя, дознавателя значительно сдвинут к окончанию производства. Чем позднее произойдет предъявление обвинения, уведомление о подозрении, тем больше времени у властного субъекта

на установление обстоятельств, подлежащих доказыванию, и невмешательство защитника в производство. Следует признать, что и следователи, и дознаватели стараются максимально отсрочить время вынесения постановления о привлечении в качестве обвиняемого и уведомления о подозрении соответственно.

Таким образом, складывается ситуация, в которой подозреваемому предоставляется больше гарантий в ходе дознания, а обвиняемому – при осуществлении предварительного следствия. Подобное закрепление в нормах уголовно-процессуального законодательства не обоснованно с практической и теоретической точек зрения и требует изменения.

Дифференциация процессуальной формы предварительного расследования не должна происходить за счет прав граждан, вводить правоприменителей в заблуждение относительно важности одних процессуальных институтов перед другими. Говоря о том, что предъявление обвинения при осуществлении предварительного следствия дает определенные гарантии обвиняемому, позволяет одновременно полагать, что лицо, в отношении которого производится дознание, этих гарантий лишено.

На основании изложенного представляется целесообразным определить необходимость существования в уголовно-процессуальном законодательстве двух статусов подозреваемого и обвиняемого и оставить одного из них в качестве единственного участника уголовного судопроизводства, в отношении которого осуществляется уголовное преследование на досудебной стадии уголовного судопроизводства. Постановка вопроса о превращении подозреваемого в главного и постоянного участника предварительного расследования во всех формах, предложения по реформированию института предъявления обвинения нашли свое отражение в научной литературе более 20 лет назад[1].

Таким образом, наиболее целесообразным в складывающейся ситуации нам видится оптимизация форм предварительного расследования посредством их приведения к единому стандарту относительно предоставления равных гарантий таким участникам

---

[1] Гаврилов Б.Я. Совершенствование досудебного производства в свете реализации основных положений УПК РФ // Уголовный процесс. 2005. № 1. С. 20; Пономаренко С.И. Современные проблемы реализации процессуального статуса подозреваемого: автореф. дис. … канд. юрид. наук. Волгоград, 2005. С. 16.

уголовного судопроизводства, как подозреваемый и обвиняемый и возможности оптимизации субинститутов уголовного преследования на стадии досудебного уголовного производства.

Список источников

1. Стенограмма конференции: «Уголовно-процессуальный кодекс Российской Федерации и проблемы правоприменительной практики» (26 февраля 2002 г.). Ярославль. 2002. 162 с.
2. Информационный сборник № 1. Материалы работы Межведомственной рабочей группы (Научно-экспертного совета) по уголовному и уголовно-процессуальному законодательству в 2004 г. Москва. 2005. 162 с.
3. Стенограмма заседания Межведомственной рабочей группы при Комитете по гражданскому, уголовному, арбитражному и процессуальному законодательству (17 февраля 2006 г.). Москва. 2006. 70 с.
4. Курс уголовного процесса / Под ред. Л.В. Головко. 2-е изд., испр. М., 2017. 1278 с.
5. Строгович М.С. Учение о материальной истине в уголовном процессе. М, 1947. 276 с.
6. Пономаренко С.И. Современные проблемы реализации процессуального статуса подозреваемого: автореф. дис. … канд. юрид. наук. Волгоград, 2005. 18 с.
7. Гаврилов Б.Я. Совершенствование досудебного производства в свете реализации основных положений УПК РФ // Уголовный процесс. 2005. № 1. С. 16–22.

В.А. Прорвич
Национальный исследовательский университет
«Высшая школа экономики»

Влияние принципа дополнительности на формирование юридических алгоритмов доказывания по уголовным делам о киберпреступлениях в сфере экстремизма

Аннотация. Высокие темпы роста киберпреступности требуют создания для оперативного выявления и своевременного пресечения таких преступлений современных информационных технологий,

выверенных с правовой точки зрения. Важную роль в формировании научного фундамента для таких разработок играет применение возможностей всех наук уголовно-правового и информационного блоков. Однако нередко приходится сталкиваться с такими проявлениями «принципа дополнительности», когда точное следование положениям уголовного права приводит к неопределенностям в применении положений информатики, и наоборот, введение в информатику правовых положений, приводит к размыванию их смыслов. Еще больше неопределенностей возникает при раскрытии бланкетных диспозиций соответствующих уголовно-правовых норм и формировании развернутой уголовно-правовой характеристики киберпреступлений в сфере экстремизма с использованием положений гражданского и специального законодательства. Проявления принципа дополнительности приводят и к возникновению ряда неопределенностей при формировании комплексных криминалистических методик с системой обратных связей для расследования киберэкстремизма различного вида, а также при применении специальных знаний судебных экспертов и специалистов для получения доказательств и доказывания с их помощью. Показаны принципиально новые возможности преодоления возникающих неопределенностей при создании необходимого высокотехнологичного инструментария на интегрированном фундаменте наук уголовно-правового и информационного блоков.

Ключевые слова: киберпреступность, киберэкстремизм, принцип дополнительности, соотношения неопределенностей, состав преступления, доказательства, предмет доказывания, пределы доказывания, юридические алгоритмы, комплексные криминалистические методики, специальные знания.

Происходящие в последние годы качественные изменения современной преступности, активно использующей современные информационные технологии не только для совершения киберпреступлений нового вида, но и для их сокрытия в искусственно созданном информационном пространстве компьютерных сетей, ставят перед юридической наукой принципиально новые задачи. К тому же, на правотворчество в данной сфере существенное влияние оказывают традиции, сложившиеся среди специалистов, разрабатывающих

информационные системы и создающих необходимое программное обеспечение, а также принятые ими правила оперирования в информационно-сетевом пространстве компьютерных сетей. Важно отметить и проявления принципа дополнительности, в связи с возникновением ряда неопределенностей при взаимном проникновении данных правил в систему уголовного правотворчества и правоприменения.

В качестве примера можно привести введение в 2019 г. системы цифровых прав как нового вида имущественных прав – обязательственных прав, содержание которых и условия их осуществления определяются в соответствии с правилами информационной системы»[1]. При этом данные правила устанавливаются обладателями этих информационных систем, а требование их обязательного соответствия действующему законодательству и указание об ответственности за его нарушение оговорено не было.

При введении понятия «цифровые финансовые активы»[2], они были определены как цифровые права, выпуск, учет и обращение которых возможны только путем внесения записей в информационной системе на основе распределенного реестра. Установлено, что они могут быть объектом залога, сделок купли-продажи, обмена одного вида цифровых финансовых активов на другой (в том числе выпущенных по правилам иностранных информационных систем) или на цифровые права иных видов. Здесь важно подчеркнуть, что правила иностранных информационных систем не связаны с российским законодательством, что вносит еще больше неопределенностей при создании системы уголовно-правовой защиты соответствующих субъектов цифровых прав.

Вместе с тем, учитывая особенности проявления принципа дополнительности, можно сделать вывод, что подобные подходы законодателя, которые привели к возникновению отмеченных выше неопределенностей, вполне соответствуют тем обычаям, которые были установлены создателями глобальной информационной сети Интернет и их пользователями. То есть, при раскрытии данных «цифровых» понятий, законодатель ввел принципиально новый вид

[1] Федеральный закон № 34-ФЗ от 18.03.2019. // СПС Консультант плюс (дата обращения 21.03.2025).

[2] Федеральный закон № 259-ФЗ от 31.07.2020. // СПС Консультант плюс (дата обращения 21.03.2025).

обязательственных прав, основанных на правилах информационных систем, учитывая сложившиеся обычаи делового оборота в данной сфере.

В «классическом» определении принципа дополнительности, введенном Нильсом Бором еще в 1927 г., точное определение местоположения микрочастицы приводит к невозможности точного определения ее скорости. Причиной этого является влияние прибора, созданного в рамках системы представлений, сложившихся в макромире, на состояние изучаемого микрообъекта, существующего по совсем другим законам микромира.

Впоследствии данный принцип приобрел более широкое, общефилософское толкование при рассмотрении взаимоисключающих понятий различных наук[1]. На его основе возможно объяснить отмеченные выше парадоксы, связанные с возникновением неопределенностей при, казалось бы, совершенно естественном дополнении системы понятий, созданных в рамках наук уголовно-правового блока, некоторыми понятиями из совершенно другого, созданного интеллектуальными усилиями представителей наук информационного блока, информационного пространства компьютерных сетей.

При этом ряд неопределенностей возникает и на уровне совместного применения положений уголовного, гражданского и специального законодательства для раскрытия бланкетных диспозиций уголовно-правовых норм по киберпреступлениям различного вида. Некоторые неопределенности проявляются при раскрытии информационно-правовой структуры и содержания понятия «доказательство», формировании криминалистической характеристики киберпреступления, применении специальных знаний для получения, проверки и оценки доказательств по соответствующим уголовным делам.

Изучение особенностей раскрытия информационно-правовой структуры характеристик киберпреступлений различного вида показывает, что при этом причиной многих юридических ошибок становится необходимость применения уголовно-правовых норм, диспозиции которых носят бланкетный, отсылочный и смешанный характер. Для формирования развернутых уголовно-правовых характеристик конкретных киберпреступлений, на основании которых

[1] Гальцов Д.В. Дополнительности принцип. / Большая Российская энциклопедия, т. 9. М.: Большая Российская энциклопедия, т. 9, С. 278-279.

создается возможность идентификации обязательных и факультативных признаков составов данных преступлений, приходится использовать раз положений гражданского и специального законодательства. Но нередко в результате таких действий оказывается, что полученная таким образом уголовно-правовая характеристика киберпреступления выходит за рамки уголовного права.

Одним из наиболее эффективных средств для профилактики подобных ошибок является раскрытие тех неопределенностей, которые характеризуют отбираемые положения гражданского и специального законодательства из-за особенностей проявления принципа дополнительности. В частности, при формировании развернутых уголовно-правовых характеристик киберпреступлений в сфере экстремизма, при раскрытии соответствующих неопределенностей учитывались те критерии, которые были использованы при классификации преступлений данного вида, выполненных совместно с В.В. Бычковым[1].

Что касается раскрытия неопределенностей, которые связаны с особенностями проявления принципа дополнительности при формировании развернутых уголовно-правовых характеристик киберпреступлений в сфере экономики и финансов, то при этом важное значение имеет выявление особенностей правил тех информационных систем, которые были использованы для формализации соответствующих правоотношений субъектов цифровых прав[2].

---

[1]Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография, под ред. В.А. Прорвича. / М.: Альпен-Принт, 2024, 572 с.; Бычков В.В., Прорвич В.А. Киберэкстремизм: понятие, квалификация, расследование: учебное пособие. / М.: Московская академия Следственного комитета России, 2023 г., 330 с.; Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети «Интернет» // Российский журнал правовых исследований. 2021. Том 8. № 1. С. 1-8; Бычков В.В., Прорвич В.А. Алгоритмы выявления признаков экстремистской и террористической деятельности с использованием Интернета на основе информационных шаблонов возможных составов преступлений данного вида // Расследование преступлений: проблемы и пути их решения. 2022. № 2. С. 43-50.

[2] Прорвич В.А. Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы // Российский журнал правовых исследований. 2023. Том 10. № 3. С. 7–19; Организация и методика расследования отдельных видов экономических преступлений: учебно-методическое пособие / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М., 2016.

Важно обратить внимание и на то, что раскрытие тех неопределенностей, которые обусловлены проявлениями принципа дополнительности, может осуществляться в рамках нескольких этапов последовательных приближений с обратными связями. На первом этапе после раскрытия данных неопределенностей в первом приближении, производится анализ полученного первого варианта развернутой уголовно-правовой характеристики конкретного киберпреступления. После выполнения его анализа на соответствие важнейшим принципам и положениям уголовного права, производится детализация тех ограничений, которые вводятся на положения гражданского и специального законодательства, используемые при раскрытии бланкетных диспозиций соответствующих уголовно-правовых норм.

Наиболее сложные ситуации возникают при раскрытии неопределенностей, связанных с правилами разнообразных информационных систем, созданных их обладателями, которые применялись субъектами киберпреступлений. В тех случаях, когда правила информационных систем соответствуют требованиям действующего законодательства, это также может быть установлено в рамках нескольких этапов последовательных приближений. Если же на определенном этапе устанавливается несоответствие таких правил требованиям действующего законодательства, то проводится более детальный анализ особенностей данных правил на предмет возможного наличия «смежного» преступления, совершенного обладателем данной информационной системы либо его соучастниками.

Подобные юридические алгоритмы, нацеленные на сопоставление содержательных особенностей положений уголовного, гражданского и специального законодательства, а также правил информационных систем, установленных их обладателями, помогают следователю выполнить анализ информации, имеющей правовой статус, применительно к конкретным следственным ситуациям. Для снижения его трудоемкости важное значение имеет формирование системы информационных эталонов, сориентированных на раскрытие указанных информационных неопределенностей применительно к каждому виду киберпреступлений[1].

Проявление принципа дополнительности создает ряд неопределенностей в части формирования предмета доказывания по

[1] Расторопов С.В., Прорвич В.А. Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2024. Том 17, № 2. С. 143–169.

уголовным делам о киберпреступлениях в сфере экстремизма и установления пределов доказывания с применением того инструментария, который был создан не только в рамках уголовно-процессуального права, но и криминалистики. Выше уже отмечалось, что в ходе расследования уголовного дела по киберпреступлениям различного вида возникает ряд информационных пробелов и неопределенностей. Поскольку в уголовно-процессуальном праве доказательства вероятностного характера не применяются, а все сомнения толкуются в пользу обвиняемого, то вполне естественным решением является применение развитого в криминалистике версионного мышления для заполнения выявленных информационных пробелов.

При формировании криминалистической характеристики киберпреступлений их уголовно-правовая характеристика дополняется системой обстоятельств, подлежащих доказыванию по соответствующим уголовным делам, а также используемыми информационными технологиями[1]. Но из-за проявлений принципа дополнительности в криминалистическую характеристику конкретного киберпреступления могут быть внесены неопределенности, которые могут по-разному влиять на те следственные ситуации, которые складываются на различных стадиях расследования уголовного дела. Это нередко приводит к необходимости выполнения дополнительных следственных действий, разработке и обоснованию новых следственных версий, а также организации их надлежащей проверки и оценки.

На основе развернутой, многосторонней и динамически адаптируемой криминалистической характеристики конкретного киберпреступления, создается ряд дополнительных возможностей и по надлежащему формированию экспертных задач. Это тем более важно, что объекты судебной экспертизы следствию приходится формировать на основе электронной документации и иной электронной информации, имеющей значение для расследуемого уголовного дела. При этом усилия следователей могут быть дополнены возможностями специалистов, обладающих необходимыми специальными знаниями и профессиональными компетенциями.

---

[1] Бессонов А.А. Технология построения типовой криминалистической характеристики преступлений // Российский следователь. 2018. № 7. С. 3–7.

Важную роль играет дополнение криминалистической методики специальным модулем, предназначенным для выполнения проверки и оценки собранных доказательств, включая установление достаточности собранной их совокупности. При этом, как уже отмечалось выше, с помощью специальных юридических алгоритмов с двойной системой юридических тождеств может быть установлена не только достаточность собранной совокупности доказательств, но и их избыточность.

В таких случаях, в криминалистической методике вводится обратная связь данного модуля с возвратом к первой части криминалистической методики, нацеленной на формирование развернутой криминалистической характеристики данного киберпреступления. С учетом сведений, содержащихся в «лишних» доказательствах, дальнейшие действия в рамках данной методики могут производиться по следующим вариантам.

В качестве первого варианта следственных действий по разрешению следственной ситуации, связанной с выявлением «лишних» доказательств по расследуемому уголовному делу, возможно формирование обоснованной версии о наличии другого, «смежного» преступления, часть признаков состава которого совпадает с первоначально идентифицированным, а другая часть – совпадает по содержанию с выявленными «лишними» доказательствами. После этого, в рамках проверки данной следственной версии, производится формирование развернутой криминалистической характеристики данного «смежного» преступления, а затем и выполнение других следственных действий, описанных выше.

В качестве второго варианта следственных действий по разрешению данной следственной ситуации, возможно формирование обоснованной версии о наличии не одного, уже расследованного преступления, а совокупности из двух преступлений. При этом часть признаков состава второго преступления совпадает по содержанию с выявленными «лишними» доказательствами. После надлежащей проверки данной следственной версии, производится формирование развернутой криминалистической характеристики второго преступления из их совершенной совокупности, а затем и выполнение других следственных действий по сбору, проверке и оценке доказательств по второму преступлению, уже описанных выше.

Здесь важно обратить внимание на то, что во многих случаях совокупность подобных киберпреступлений совершается группой лиц, с различными, в том числе, «перекрестными» формами соучастия. Поэтому в рамках данной комплексной криминалистической методики выполняется ряд следственных действий, нацеленных на выделение составов преступлений, совершенных каждым из соучастников. Для этого предусмотрено применение данной методики в рамках циклического алгоритма выполнения соответствующих следственных действий[1].

Завершающая часть данной комплексной криминалистической методики призвана дополнить следственные действия по раскрытию и расследованию киберпреступлений в сфере экстремизма, действиями иного характера, нацеленными на профилактику данных преступлений и их совокупностей с различными формами соучастия. В рамках данной части кроме «традиционных» средств криминалистической профилактики преступлений раскрыт ряд возможностей многоступенчатой профилактики киберпреступлений.

В ее основу заложено раскрытие особенностей установления уголовной ответственности за совершение киберпреступлений в сфере экстремизма, предусмотренных «привилегированными» уголовно-правовыми нормами. При этом важно учитывать, что освобождение от уголовной ответственности в соответствии с данными уголовно-правовыми нормами не происходит «автоматически». Для реализации тех возможностей, которые предусмотрены законодателем, следствию необходимо собрать определенную совокупность доказательств, причем, не только применительно к установлению состава преступления субъекта «основного» преступления, предусматривающего освобождение от уголовной ответственности при соблюдении определенных условий, но и состава второго преступления, совершенного им в соучастии.

Результаты проведенных исследований показывают, что не менее серьезные проблемы борьбы с киберпреступлениями различного вида

[1] Бычков В.В., Прорвич В.А. Особенности циклического алгоритма выполнения следственных действий при расследовании совокупностей преступлений в сфере киберэкстремизма с различными формами соучастия. // Расследование преступлений: проблемы и пути их решения, № 4, 2023, с. 98–103; Бычков В.В., Прорвич В.А. Информационная модель криминалистической характеристики киберэкстремизма. // Вестник Московской академии Следственного комитета Российской Федерации. № 3, 2023. С. 113–120.

связаны с тем, что производство большей части следственных действий связано с обработкой электронных документов и иной электронной информацией из материалов уголовного дела. Важно учитывать, что события таких преступлений происходят в искусственно созданном интеллектуальными усилиями ученых и специалистов в сфере прикладной математики и кибернетики информационном пространстве компьютерных сетей, которое имеет мало общего с привычным для юристов материальным миром. При этом компьютер, смартфон либо иное компьютеризованное устройство воспринимается их пользователями чаще всего, как многие другие электронные приборы, а информацию, отправленную или полученную в виде текста или изображения, как вполне однозначно характеризующую события в материальном мире.

Представители служб информационной и компьютерной безопасности фирм, предоставляющих широкий спектр самых разнообразных услуг пользователям смартфонов и компьютеризованных устройств, воспринимают данные устройства совершенно иначе. Они прекрасно разбираются не только в особенностях организации потоков информации, управления определенными каналами связи. Не менее важно понимание ее уязвимости к внешнему воздействию с помощью вредоносной информации, компьютерных программ, а также сфокусированных на определенных информационных системах интенсивных потоков электронных данных. Это позволяет им использовать различные программные средства для защиты соответствующих технических устройств от проникновения в них вредоносных компьютерных программ, несанкционированного доступа к информации, создаваемой, хранящейся и преобразующейся в установленном порядке в различных информационных системах.

Представители государственных ведомств, ответственных за создание и развитие данного информационного пространства, исходя из важнейших интересов нашего государства и общества, выполняющие широкий спектр задач по регулированию деятельности субъектов различного вида и уровня в данной сфере, обладают еще более широким и глубоким, системным представлением о сходстве и различиях данного пространства с материальным миром. В том числе, речь идет не только о характере широчайшего спектра услуг, предоставляемых пользователям разнообразных смартфонов и иных гаджетов, но и тяжелейших последствиях от деятельности

определенных субъектов в данном искусственно созданном информационном пространстве, связанных с искусственно созданными техногенными катастрофами различного характера и масштабов.

Поэтому представители государственной власти уделяют значительное внимание правовой регламентации деятельности субъектов различного вида и уровня в данном искусственно созданном информационном пространстве компьютерных сетей. Можно привести многочисленные примеры законотворческой деятельности в данной сфере, а также принятие ряда подзаконных актов, раскрывающих необходимые детали правового регулирования правоотношений в сфере, искусственно созданной интеллектуальными усилиями весьма ограниченного круга ученых и специалистов из разных стран.

В качестве одного из них достаточно обратить внимание на содержание постановления Правительства РФ и ведомственного нормативного акта Роскомнадзора, раскрывающих особенности структуры искусственно созданного информационного пространства компьютерных сетей, установленного порядка получения доступа к его структурным элементам, а также введенные при этом ограничения и запреты[1].

Представители правоохранительных органов, перед которыми ставятся задачи по оперативному выявлению, своевременному раскрытию и надлежащему расследованию киберпреступлений различного вида, совершенных в искусственном информационном

---

[1] Постановление Правительства РФ от 26.10.2012 № 1101 (ред. от 29.04.2023) «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // Собрание законодательства РФ. 2012. № 44. Ст. 6044; Приказ Роскомнадзора от 21.02.2013 № 169 (ред. от 09.03.2022) «Об утверждении Порядка получения доступа к содержащейся в единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет» // Российская газета. 2013. 5 апреля.

пространстве компьютерных сетей, а также по их многоступенчатой профилактике, сталкиваются с необходимостью создания информационных технологий нового вида, выверенных с правовой точки зрения. При этом уже на самых первых шагах своего общения со специалистами по информатике и программированию они сталкиваются с тем, что ставшие давно привычными для них представления о преступлениях и преступниках созданные в рамках криминологии, криминалистики и других наук уголовно-правового блока, имеют мало общего с тем языком и способом мышления, которые характерны для представителей наук информационного блока.

В отличие от давно сложившихся представлений юристов о материальном мире и идеальном его отражении в сознании законопослушных граждан и преступников, а также о формировании «механизма» преступления и процессах следообразования в ходе приготовления преступления определенного вида, его совершения и сокрытия, в искусственно созданном информационном пространстве речь идет о совсем другом виде идеального, связанном с особенностями интеллектуальной деятельности «незначительной» в количественном плане, но способной увлечь все человеческое общество в данное пространство группы ученых высшей квалификации в сфере прикладной математики и кибернетики.

Важно подчеркнуть, что данное искусственное информационное пространство создавалось не одномоментно, а в течение достаточно длительного времени, впитывая в себя те новые возможности, которые создавались развивающимися параллельно прикладной математикой, кибернетикой и информатикой. Сформированное в их рамках новое научное направление – киберлингвистика, позволила вывести на принципиально новый уровень те возможности, которые дает взаимодействие человека с компьютером с использованием широкого спектра искусственных алгоритмических языков.

Учитывая неразрывные связи языка и мышления человека, важно обратить внимание на то, что, судя по доступным публикациям, среди создателей данного информационного пространства юристы высшей квалификации, понимающие язык и способ мышления ученых с специалистов в сфере информационного блока, отсутствовали. Более того, в последние годы все более активно среди юристов используются разнообразные «цифровые понятия», не имеющие никакого отношения ни к математике, ни к наукам уголовно-правового блока, и лишь провоцирующие совершение юридических ошибок.

Фактически, тем самым создается видимость «осовременивания» понятийного аппарата юридических наук, что не только не отражает стремление ведущих ученых получить хотя бы элементарные представления о современной математике, кибернетике и информатике, но и приводит к опасным заблуждениям относительно способа мышления современных преступников. Это стало одной из причин высочайшего уровня латентности киберпреступлений различного вида, наносящих крупный ущерб гражданам, для снижения которого принимаются экстренные меры на законотворческом, организационном и информационно-технологическом уровнях.

Вполне очевидной альтернативой данной «цифровой суете» может стать создание современного юридического алгоритмического языка, позволяющего повысить уровень взаимопонимания юристов с представителями наук информационного блока. Необходимо напомнить, что во время празднования 300-летия Российской академии наук, на встрече с президентом страны В.В. Путиным ведущие ученые в качестве главной проблемы указали на необходимость введения куса математики при обучении юристов. Это позволяет создать основы для формирования нового научного направления – уголовно-правовой информатики, нацеленного на раскрытие важнейших особенностей современной киберпреступности и разработку эффективных средств борьбы с ней.

В рамках данного направления создаются и принципиально новые возможности для раскрытия тех неопределенностей, которые возникают из-за описанных выше проявлений принципа дополнительности при взаимопроникновении наук уголовно-правового и информационного блоков. Ряд таких возможностей уже был продемонстрирован при создании иерархических систем юридических алгоритмов и информационных эталонов.

Достаточно серьезный задел в создании научного фундамента для разработки современного информационно-технологического инструментария, обеспечивающего возможность оперативного выявления, своевременного раскрытия и надлежащего расследования киберпреступлений в сфере экстремизма был создан в рамках наших совместных исследований с В.В. Бычковым, результаты которых были

обобщены в недавно опубликованной монографии[1]. Эти заделы охватывают весь комплекс проблем, начиная с раскрытия особенностей уголовно-правовых характеристик киберпреступлений в сфере экстремизма, создания системы юридических алгоритмов для надлежащей формализации признаков составов преступлений, идентификации информационно-правовой структуры доказательств, их проверки и оценки, а также установления достаточности их собранной совокупности. Важно учитывать и специфику разработанных комплексных криминалистических методик с циклическими обратными связями, позволяющими выделить составы преступлений каждого из соучастников совершенных совокупностей преступлений в сфере киберэкстремизма.

Результаты проведенных исследований позволили сделать вывод о том, что для оперативного выявления, своевременного раскрытия и надлежащего расследования киберпреступлений в сфере экстремизма возможно в кратчайшие сроки создать современный высокотехнологичный инструментарий на основе проблемно-ориентированного программного обеспечения, сориентированного на его применение в рамках интерактивных информационных систем.

Список источников

1. Бессонов А.А. Технология построения типовой криминалистической характеристики преступлений // Российский следователь. 2018. № 7. С. 3–7.

2. Бычков В.В., Прорвич В.А. Киберэкстремизм: понятие, квалификация, расследование: учебное пособие. М.: Московская академия Следственного комитета России, 2023.

3. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография, под ред. В.А. Прорвича. М.: Альпен-Принт, 2024.

4. Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети Интернет // Российский журнал правовых исследований. 2021. Том 8. № 1. С. 1–8.

[1] Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография, под ред. В.А. Прорвича. М.: Альпен-Принт, 2024, 572 с.

5. Бычков В.В., Прорвич В.А. Алгоритмы выявления признаков экстремистской и террористической деятельности с использованием Интернета на основе информационных шаблонов возможных составов преступлений данного вида // Расследование преступлений: проблемы и пути их решения. 2022. № 2. С. 43–50.
6. Бычков В.В., Прорвич В.А. Особенности циклического алгоритма выполнения следственных действий при расследовании совокупностей преступлений в сфере киберэкстремизма с различными формами соучастия. // Расследование преступлений: проблемы и пути их решения, № 4, 2023. С. 98–103.
7. Бычков В.В., Прорвич В.А. Информационная модель криминалистической характеристики киберэкстремизма. // Вестник Московской академии Следственного комитета Российской Федерации. № 3, 2023. С. 113–120.
8. Новиков А.М., Прорвич В.А. Доказательства и доказывание в следственной практике. М.: Московская академия Следственного комитета России, 2022.
9. Прорвич В.А. Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы. / Российский журнал правовых исследований. 2023. Том 10. № 3. С. 7–19.
10. Прорвич В.А. Научные и организационные основы государственной программы борьбы с киберэкстремизмом: творческое наследие Василия Васильевича Бычкова // Расследование преступлений: проблемы и пути их решения. № 1, 2024. С. 187–198.
11. Расторопов С.В., Прорвич В.А. Информационные основы современной уголовно-правовой защиты субъектов цифровой экономики и финансов // Право. Журнал Высшей школы экономики. 2024. Том 17, № 2. С. 143–169;

И.М. Пшеничнов
Санкт-Петербургская академия
Следственного комитета

Противодействие киберэкстремизму в современных социально-правовых реалиях

Аннотация. В данной статье рассматривается проблема киберэкстремизма как одной из наиболее актуальных угроз в современных социально-правовых реалиях. Актуальность исследования вызвана стремительным развитием технологий и распространением сети Интернет, которые предоставляют экстремистским группировкам новые платформы для пропаганды и вербовки. Статья раскрывает проблематику современных проявлений киберэкстремизма, включая использование социальных сетей, мессенджеров, а также других цифровых инструментов для распространения радикальных идей и практик.

Ключевые слова: киберэкстремизм, радикализация, противодействие, информация, ответственность, уголовный закон.

Эволюция глобальной информационной среды радикально изменила механизмы распространения экстремистских идей, превратив виртуальное пространство в одну из ключевых платформ для вербовки, координации и финансирования противоправной деятельности. В современных условиях экстремизм, опосредованный использованием цифровых технологий, утратил традиционные пространственные и временные ограничения, приобретя характер гибридной угрозы, сочетающей в себе элементы идеологической пропаганды, сетевой мобилизации и киберпреступности.

В результате всего этого мы имеем перед собой феномен киберэкстремизма, который выходит за пределы локальных юрисдикций государств, формируя транснациональные сети, действующие с высокой степенью анонимности и децентрализации. С учетом чего вполне закономерно, что Президент Российской Федерации В. В. Путин акцентирует внимание на особой значимости деятельности по выявлению и пресечению преступных действий лиц, использующих сеть Интернет в целях осуществления пропаганды

распространения деструктивных идеологий, раскола и ослабления нашего общества[1]. В свою очередь, как указывается в докладе Европола “Internet Organised Crime Threat Assessment (IOCTA) 2023”, соответствующие группировки «все чаще используют инновационные технологии для координации действий и вербовки новых членов, применяя зашифрованные каналы связи и анонимные платформы для обхода существующих правоохранительных механизмов»[2]. Тогда как популярность, распространенность и доступность интернет-мессенджеров, а также высокий уровень анонимизации их пользователей обеспечивают условия для радикализации, в том числе и подростковой среды[3], что свидетельствует о формировании крайне высокого уровня угрозы для конституционной безопасности.

Актуальность научного осмысления представленной проблематики обусловлена не только стремительным ростом делинквентной активности в сети, но и недостаточной эффективностью уголовно-правовых механизмов пресечения подобных деяний. Наличие значительных правовых пробелов, размытость дефиниций и различия в интернациональных подходах к юридической оценке соответствующего явления снижают эффективность правоприменения[4] и требуют комплексного междисциплинарного

---

[1] Выступление Президента Рос. Федерации В. В. Путина на расширенном заседании коллегии ФСБ России (28 февраля 2023 года). Сайт Президента России. Режим доступа: http://www.kremlin.ru/events/president/news/70597 (дата обращения 17 апреля 2025 года).

[2] Internet Organised Crime Threat Assessment (IOCTA) 2023. *European Union Agency for Law Enforcement Cooperation*. Luxembourg: Publications Office of the European Union, 2023. Режим доступа: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf (дата обращения 17 апреля 2025 года).

[3] Клещина Е.Н., Байханов А.И. О некоторых вопросах организации профилактической работы с подростковым экстремизмом, совершаемым посредством использования информационно-телекоммуникационных технологий // Организация работы по предупреждению деструктивной идеологии в подростковой среде: материалы научно-практической конференции (Москва, 20 декабря 2024 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. С. 44.

[4] Бычков В.В. К вопросу о назначении комплексных лингвистических экспертиз при расследовании киберэкстремизма // Актуальные вопросы профилактики и расследования преступлений экстремистской и террористической направленности: материалы Международной научно-практической

анализа. В этом контексте противодействие ему становится одной из приоритетных задач современной уголовно-правовой политики и международного сотрудничества.

Сущностно киберэкстремизм представляет собой трансформацию традиционных форм радикализма, адаптированных к возможностям современной цифровой среды. Он охватывает широкий спектр действий: от распространения идеологической пропаганды до вербовки новых участников, координации противоправной деятельности и финансирования террористических операций посредством онлайн-платформ. В отличие от классических форм проявления экстремизма, инновационные технологии обеспечивают высокую скорость распространения деструктивных материалов, анонимность и возможность трансграничного взаимодействия без физического контакта, что не может не сказываться и на аспектах более частного теоретико-прикладного характера.

В частности, в результате фигурирующих в настоящем контексте процессов происходит трансформация уже устоявшихся в уголовно-правовой доктрине подходов к пониманию информации, как одного из элементов состава преступления. В частности, наиболее распространенной исследовательской позицией здесь выступает определение предмета преступления, как материального субстрата, элемента материального мира, в связи с которым или по поводу которого совершается преступление, на который непосредственно воздействует виновное лицо[1]. Однако содержание интересующей нас категории (от лат. *informatio* – «разъяснение, изложение») свидетельствует о том, что она может описывать и взаимодействовать с материальным миром, но это еще не говорит о возможности ее отнесения к нему, поскольку в действительности речь ведется о «сведениях (сообщениях, данных) независимо от формы их представления»[2]. Справедливости ради стоит отметить, что в современных разработках встречаются попытки адаптировать обозначенную дефиницию к изменившимся социально-правовым реалиям, однако и они не в полной мере лишены определенного рода

конференции (Екатеринбург, 9 ноября 2023 года). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 32.

[1] См.: Состав преступления: учебник для вузов / под редакцией Е. В. Фоменко. Москва: Издательство Юрайт, 2025. С. 45.

[2] Тихомирова Л.В., Тихомиров М.Ю. Юридическая энциклопедия. 6-е изд., доп. и перераб. М.: Изд. Тихомирова М. Ю., 2009. С. 400.

противоречий и недостатков, в выражающихся в отнесении информационных единиц на соответствующем носителе к вещам материального мира[1]. В частности, при таком подходе возникает закономерный вопрос о предмете общественно опасного деяния предусмотренного, например, статьей 207[3] УК РФ, в рамках которого представляется, что таковым выступают именно достоверные сведения о Вооруженных Силах Российской Федерации, которые объективно «не привязаны» к какому-либо материальному носителю. Напротив этого заведомо ложные сообщения следует расценивать никак иначе чем орудие преступления, поскольку используются для воздействия на объект посягательства. С учетом чего в соответствующих случаях несколько некорректными представляются судебные решения об уничтожении компьютера, в связи с признанием его орудием преступления[2].

Киберэкстремизм в современных условиях выступает одной из наиболее сложных форм преступной деятельности, адаптированной к возможностям цифровой среды. Его транснациональный характер, высокая латентность и оперативность распространения требуют переосмысления традиционных уголовно-правовых подходов, которые уже сегодня вполне отчетливо демонстрируют определенный уровень неоптимизированности. Тогда как действующее регулирование противодействия обозначенному деструктивному явлению остается фрагментарным и не полностью учитывает специфику цифровых коммуникаций. Сложности квалификации деяний, необходимость защиты свободы выражения мнений и расхождения в правовых взглядах на интернациональном уровне создают дополнительные вызовы. В свою очередь эффективное противодействие подобным проявлениям радикализации общественных отношений возможно лишь при комплексном подходе, включающем совершенствование национальных уголовных норм, развитие превентивных мер и укрепление механизмов международного сотрудничества в условиях цифровой глобализации.

---

[1] Сверчков, В. В. Уголовное право. Общая часть: учебник для вузов / В.В. Сверчков. – 12-е изд., перераб. и доп. – М.: Юрайт, 2025. С. 100.

[2] Суд в Казани постановил уничтожить компьютер блогера как орудие преступления // Интернет-издание «Газета.Ru», 2011. 9 июня. URL: https://www.gazeta.ru/news/blogs/2011/06/09/n_1876785.shtml?ysclid=m9zu6bm731806744632 (дата обращения 17 апреля 2025 г.).

Список источников

1. Бычков В.В. К вопросу о назначении комплексных лингвистических экспертиз при расследовании киберэкстремизма / В. В. Бычков // Актуальные вопросы профилактики и расследования преступлений экстремистской и террористической направленности: материалы Международной научно-практической конференции (Екатеринбург, 9 ноября 2023 года). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 31–36.

2. Клещина Е.Н., Байханов А.И. О некоторых вопросах организации профилактической работы с подростковым экстремизмом, совершаемым посредством использования информационно-телекоммуникационных технологий // Организация работы по предупреждению деструктивной идеологии в подростковой среде: материалы научно-практической конференции (Москва, 20 декабря 2024 г.). М.: Московская академия Следственного комитета имени А. Я. Сухарева, 2025. С. 39–45.

3. Сверчков, В.В. Уголовное право. Общая часть: учебник для вузов/в. – 12-е изд., перераб. и доп. – М.: Издательство Юрайт, 2025. 332 с.

4. Состав преступления: учебник для вузов / под редакцией Е. В. Фоменко. Москва: Издательство Юрайт, 2025. 153 с.

5. Суд в Казани постановил уничтожить компьютер блогера как орудие преступления // Интернет-издание Газета.Ru, 2011. 9 июня. https://www.gazeta.ru/news/blogs/2011/06/09/n_1876785.shtml?ysclid=m9zu6bm731806744632 (дата обращения 17 апреля 2025 года).

6. Тихомирова Л.В., Тихомиров М.Ю. Юридическая энциклопедия. 6-е изд., доп. и перераб. М.: Изд. Тихомирова М.Ю., 2009. С. 400. 1088 с.

В.В. Решетихин
Санкт-Петербургская академия Следственного комитета

Методика использования специальных знаний при расследовании киберпреступлений экстремистской направленности: современные вызовы и перспективы

Аннотация. В условиях цифровой трансформации и роста угроз экстремизма в киберпространстве расследование соответствующих преступлений требует применения инновационных методик и специальных знаний. Данная работа посвящена анализу современных подходов к использованию экспертных компетенций в области цифроой криминалистики, информационных технологий и права при раскрытии киберпреступлений экстремистской направленности.

Ключевые слова: методика, киберэкстремизм, расследование, мессенджеры, Интернет, программное обеспечение, искусственный интеллект, IT сфера.

В условиях стремительного развития цифровых технологий и повсеместного доступа к информации киберпреступность превратилась в ключевую угрозу для безопасности, как отдельных государств, так и мирового сообщества в целом. Особую тревогу вызывают противоправные действия экстремистского характера, реализуемые через Интернет. Подобные акты не только способствуют популяризации радикальных взглядов, но и становятся инструментом привлечения сторонников, финансирования незаконных группировок и планирования их операций. В связи с этим раскрытие таких преступлений невозможно без привлечения узкоспециализированных навыков, направленных на обнаружение, сохранение и изучение электронных улик.

Так, злоумышленники всё чаще прибегают к инструментам, скрывающим их личность. Таковыми в современном мире являются: анонимные сети по типу Tor, VPN-сервисам, цифровым валютам, а также к мессенджерам (по типу Телеграмм), с повышенной защитой данных. Поэтому стоит отметить, что средства осложняют установление личности преступников их местонахождения и как итог возникает проблема в расследовании таких видов преступлений. Ко

всему, прочему дополнительную сложность и создают методы сокрытия данных, такие как, например, внедрение информации в медиафайлы через стеганографию, то есть некое сокрытие, скрытие информации в изображениях или аудиофайлах.

Поэтому как итог следует создавать и совершенствовать программное обеспечение по выявлению и обходу таких средств непосредственно правоохранительными органами.

Далее стоит затронуть определенную трансконтинентальную специфику совершения преступлений такого характера. Так, подобные преступления часто затрагивают несколько юрисдикций, таких как: организаторы, такого рода преступлений руководят, контролируют и отдают «приказы», по совершению киберпреступлений, из одного региона, компьютерные серверы благодаря которым осуществляются и воплощаются в жизнь киберпреступления, могут размещаться в другом регионе, стране, а пострадавшие от действий такой запутанной схеме, могут находится в третьем регионе или стране. Поэтому, это усложняет и вынуждает правоохранительные органы разных стран координировать усилия между собой, но здесь же возникают нюансы, выражающиеся в частом торможении сотрудничества по разным причинам: из-за правовых коллизий и административных (бюрократических) накладок.

Поэтому, здесь же возникает вторая проблема слабо раскрываемости и практически не раскрываемости такого рода преступлений.

Также, через социальные сети и различные мессенджеры, которые были перечислены выше, экстремисты оперативно распространяют пропаганду, руководства по созданию опасных веществ и иную запрещенную информацию. Пропаганда в преступлениях экстремизма является основополагающей, так как она непосредственно действует на сознание человека. В следствии, чего человек становится объектом для совершения такого рода и вида преступлений. Поэтому, незначительное промедление в блокировке, такого контента способно привести к масштабным последствиям.

Следующим стоит затронуть нехватку специалистов в области обеспечения и противодействия киберпреступности. Так, работа с цифровыми уликами требует от специалистов компетенций не только в большой степени в IT-сфере, но и в юриспруденции по знанию базовых норм уголовного и уголовно-процессуального кодекса, а

также базовых знаний в криминалистике. Поэтому, к большому сожалению, многие ведомства сталкиваются с нехваткой таких кадров, владеющих актуальными методами анализа данных и обладающими профессиональными знаниями в IT сфере и базовых знаний в юриспруденции.

Выделив основные проблемы, на наш взгляд основополагающей темы в настоящее время, стоит определить и выявить аспектность решения таких проблем.

Так, эффективное расследование киберпреступлений, предполагает многоэтапную стратегию.

На наш взгляд, необходимо начать со сбора улик, так как данный элемент является основным костяком, в расследовании киберпреступлений.

На начальной стадии критически важно корректно извлечь электронные данные, гарантируя их допустимость в суде. Для этого используют программное обеспечение, для создания цифровых копий носителей (например, EnCase), строго соблюдая нормы уголовно-процессуального кодекса.

Так, Собранные данные анализируют с помощью профильных программ, включая: Поиск терминов, ассоциирующихся с экстремизмом. Изучение метаданных (дата создания файлов, авторство). Мониторинг сетевой активности для выявления источников. Дешифрацию скрытой информации.

Далее, стоит рассмотреть, современные алгоритмы искусственного интеллекта и машинного обучения, которые ускоряют обработку массивов данных, выявляя модели поведения экстремистов или распознавая запрещенный контент через анализ мультимедии.

Помощь специалистов также является наиболее важной перспективой для развития методики расследования преступлений в сфере киберэкстремизма. Так, криминалисты восстанавливают удаленные файлы, исследуют структуру данных и устанавливают взаимосвязи между уликами, представляя выводы в форме, доступной для судебных органов.

Не стоит забывать и о международном сотрудничестве с иностранными коллегами через Интерпол, а также проведение совместных операций помогают преодолеть трансграничные барьеры.

Поэтому, стоит как можно больше развивать инновационные инструменты анализа. Внедрение продвинутых систем на базе

искусственного интеллекта, которые способных прогнозировать кибератаки и идентифицировать угрозы на этапе их формирования, окажут огромное влияние на расследовании киберэкстремизма в том, что ускорится и упростится работа по выявлению пропагандистских материалов экстремизма.

Также, обучение специалистов в этой области путем расширения программ подготовки кадров, включая освоение новых технологий и правовых аспектов цифровой криминалистики, в дальнейшем поможет качественно расследовать преступления киберэкстремизма.

Как итог стоит сделать вывод о том, что противодействие экстремизму в цифровой среде, прежде всего, требует интеграционных технологических решений, профессиональной экспертизы и межгосударственной координации. Развитие методов анализа данных, подготовка квалифицированных кадров и совершенствование правовой базы позволят правоохранительным структурам адаптироваться к динамично меняющимся угрозам, минимизируя риски для общества, и как в дальнейшем итог раскрытие и расследовании данной категории преступлений, которые так или иначе подрывают государственный строй любой страны.

Список источников

1. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / И.Г. Смирнова и др.; науч. ред. И.Г. Смирнова. М.: Юрлитинформ, 2016.

2. Акименко М.А. О некоторых правовых и организационных аспектах предупреждения киберэкстремизма // Евразийская адвокатура. – 2025. №1(72). – С. 110.

3. Панталева Н.С., Пархитько Н.П. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. – 2020. №1. С. 47–50.

А.Ж. Саркисян
Московская академия Следственного комитета
имени А.Я. Сухарева

Основы предупреждения экстремизма и терроризма в сети интернет: заветы В.В. Бычкова

Аннотация. В статье анализируется научное наследие В.В. Бычкова в области предупреждения экстремизма и терроризма в сети Интернет. Рассмотрены концептуальные основы киберэкстремизма, методологические принципы мониторинга интернет-пространства, роль искусственного интеллекта в борьбе с экстремистскими угрозами. Представлены организационно-тактические аспекты противодействия и перспективы развития системы предупреждения. Научные разработки Бычкова сохраняют актуальность для современных правоохранительных органов.

Ключевые слова: киберэкстремизм, терроризм, интернет-безопасность, искусственный интеллект, мониторинг, профилактика, В.В. Бычков, электронное следообразование, оперативно-разыскная деятельность.

Проблема предупреждения экстремизма и терроризма в цифровом пространстве приобретает особую актуальность в современных условиях развития информационных технологий. Почетным профессором Московской академии, почетным сотрудником Следственного комитета Российской Федерации В.В. Бычковым разработана комплексная система теоретических и практических подходов к борьбе с данными угрозами[1]. Его научные труды представляют собой фундаментальный вклад в криминологическую теорию предупреждения киберэкстремизма и формируют методологическую основу для современных правоохранительных органов.

В своей базовой работе «Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской

[1] Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Академии Следственного комитета Российской Федерации. 2020. № 3(25). С. 43–46.

направленности» В.В. Бычков определил фундаментальные характеристики современного киберэкстремизма[1]. Ученый выделил ключевые особенности использования интернет-пространства экстремистами: анонимность и псевдонимность, позволяющие скрывать истинную личность организаторов; глобальный охват аудитории без географических ограничений; низкие материальные затраты на распространение экстремистского контента; высокую скорость распространения информации; возможность создания закрытых сообществ для координации противоправной деятельности.

Революционным вкладом В.В. Бычкова в теорию предупреждения киберэкстремизма стала разработка концепции электронного следообразования. В работе, написанной совместно с В.Б. Веховым, ученый ввел в научный оборот понятие электронных следов, которые могут быть использованы для выявления и расследования преступлений экстремистской направленности[2]. Василий Васильевич выделил несколько типов электронных следов: метаданные – информация о времени, месте и способе создания цифрового контента; журналы активности – записи о действиях пользователей в различных системах; сетевая активность – данные о трафике и соединениях; социальные следы – связи между пользователями и их взаимодействия.

Особое значение в научном наследии В.В. Бычкова занимает концепция использования искусственного интеллекта в борьбе с киберэкстремизмом. В работе «Искусственный интеллект как средство противодействия преступлениям экстремистской направленности», написанной совместно с В.А. Прорвичем, ученый обосновал необходимость внедрения ИИ-технологий на всех этапах противодействия экстремизму[3]. Основные направления применения ИИ включают автоматическое распознавание экстремистских материалов с использованием нейронных сетей; анализ социальных

---

[1] Там же.

[2] Бычков В.В. Электронное следообразование преступной деятельности в сети Интернет // Расследование преступлений: проблемы и пути их решения. 2020. № 1(27). С. 106–111.

[3] Бычков В.В. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет / В.В. Бычков, В.А. Прорвич // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4 (26). С. 47–52.

связей для выявления скрытых экстремистских сообществ; прогнозирование экстремистской активности на основе поведенческих паттернов; автоматическую генерацию контент-аргументов для противодействия экстремистской пропаганде.

В.В. Бычков разработал концепцию многоуровневого мониторинга интернет-пространства для выявления экстремистских проявлений[1]. Его подход предполагает автоматизированный скрининг с использованием специализированных программ для поиска потенциально опасного контента; экспертный анализ с привлечением специалистов различного профиля для оценки выявленных материалов; оперативное реагирование с немедленным принятием мер по блокированию противоправного контента.

Василий Васильевич является пионером в разработке формализованных алгоритмов для расследования «высокотехнологичных» преступлений экстремистского характера[2]. Его методология включает семь групп алгоритмов: идентификации обязательных и факультативных признаков составов преступлений; планирования следственных действий; оценки доказательств и их допустимости; взаимодействия с экспертными учреждениями; международного сотрудничества; профилактической работы; контроля качества расследования.

В фундаментальной работе по оперативно-разыскному обеспечению Бычков детально разработал систему оперативно-разыскного сопровождения борьбы с киберэкстремизмом[3]. Ключевые принципы ОРД включают превентивность – опережающее выявление экстремистских намерений; системность – комплексное использование возможностей оперативно-разыскного законодательства; технологичность – активное применение специальных технических средств; межведомственность – координацию действий различных правоохранительных структур.

---

[1] Бычков В.В. Особенности организации и научно-методического обеспечения оперативно-разыскной деятельности при раскрытии и расследовании преступлений экстремистского характера, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе Интернета / В.В. Бычков, В.А. Прорвич // Вестник Московского университета МВД России. 2021. № 4. С. 149–155.

[2] Там же.

[3] Там же.

В.В. Бычков подчеркивает транснациональный характер современного киберэкстремизма и необходимость международного сотрудничества в борьбе с ним[1]. Он выделяет следующие направления международного взаимодействия: создание единой системы обмена информацией о экстремистских угрозах между правоохранительными органами различных стран; гармонизацию национальных антиэкстремистских законодательств для исключения правовых лакун; создание международных оперативных групп для проведения совместных операций против транснациональных экстремистских сетей.

В поздних работах В.В. Бычков прогнозировал эволюцию экстремистских угроз в цифровом пространстве. Он предупреждал о возможности использования экстремистами искусственного интеллекта для создания пропагандистского контента; блокчейн-технологий для анонимного финансирования; квантовых вычислений для преодоления систем защиты; технологий дополненной и виртуальной реальности для индоктринации[2].

Бычков предлагал несколько стратегических направлений развития системы предупреждения киберэкстремизма: создание единой информационной системы мониторинга экстремистских угроз; подготовку специализированных кадров; развитие международного сотрудничества; совершенствование правовой базы; внедрение превентивных технологий на основе искусственного интеллекта.

Научное наследие В.В. Бычкова в области предупреждения экстремизма и терроризма в сети Интернет представляет собой целостную концепцию противодействия цифровым угрозам. Его подход отличается системностью, практической направленностью, инновационностью и междисциплинарностью. Основные «заветы» В.В. Бычкова могут быть сформулированы как требования технологического опережения, системного подхода, международного

---

[1] Бычков В.В. Противодействие новым вызовам экстремистской деятельности с использованием информационно-сетевых технологий на уровне трансграничных экстремистских сообществ // Вестник Московского университета МВД России. 2022. № 5. С. 54–60.

[2] Бычков В.В. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием интернета / В.В. Бычков, В.А. Прорвич // Правопорядок: история, теория, практика. 2021. № 2(29). С. 92–97.

сотрудничества, профилактической направленности и постоянного совершенствования системы противодействия.

Работы В.В. Бычкова сохраняют актуальность для современных правоохранительных органов. Его теоретические разработки и практические рекомендации должны служить ориентиром для дальнейшего развития системы национальной безопасности в цифровую эпоху.

Список источников

1. Бычков В.В. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием интернета / В.В. Бычков, В.А. Прорвич // Правопорядок: история, теория, практика. 2021. № 2(29). С. 92–97.
2. Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Академии Следственного комитета Российской Федерации. 2020. № 3(25). С. 43–46.
3. Бычков В.В. Электронное следообразование преступной деятельности в сети Интернет / В.В. Бычков, В.Б. Вехов // Расследование преступлений: проблемы и пути их решения. 2020. № 1(27). С. 106–111.
4. Бычков В.В. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет / В.В. Бычков, В.А. Прорвич // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4(26). С. 47–52.
5. Бычков В.В. Особенности организации и научно-методического обеспечения оперативно-разыскной деятельности при раскрытии и расследовании преступлений экстремистского характера, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе Интернета / В.В. Бычков, В.А. Прорвич // Вестник Московского университета МВД России. 2021. № 4. С. 149–155.
6. Бычков В.В. Противодействие новым вызовам экстремистской деятельности с использованием информационно-сетевых технологий на уровне трансграничных экстремистских сообществ / В.В. Бычков,

В.А. Прорвич // Вестник Московского университета МВД России. 2022. № 5. С. 54–60.

В.М. Шашков
Следственный комитет Российской Федерации

Расследование уголовных дел о деятельности экстремистов и террористов, применяющих криптовалюты: проблемы и пути их решения.

Аннотация. В приведенной статье автор описывает и характеризует ряд некоторых особенностей использования криптовалют в деятельности лиц, совершающих преступлений в сети интернет

Ключевые слова: киберпреступность, криптовалюта как средство совершения преступления

Криптовалюты предоставляют высокий уровень анонимности и независимы от государственных и банковских систем, что делает их привлекательными для киберэкстремистов и террористических организаций. При этом технология блокчейн обеспечивает децентрализованный характер транзакций, что затрудняет отслеживание и блокировку финансовых потоков.

В данной связи криптовалюты активно используются для финансирования террористических и экстремистских организаций, поскольку позволяют скрыть источники и направления денежных потоков.

Биткоин и другие криптовалюты стали излюбленным средством расчетов на теневых рынках даркнета, где киберэкстремисты могут приобретать оружие, наркотики, услуги киллеров и другое[1].

Исследователями выделены некоторые особенности, благодаря которым криптовалюта привлекает внимание участников

[1] Баранов В.В. Некоторые аспекты противодействия финансированию экстремизма в условиях цифровой трансформации общества // Право и государство: теория и практика. 2023. № 10(226). С. 217–219.

деятельности, связанной с финансированием экстремизма и терроризма:

– транзакции, при которых платежным средством выступает криптовалюта, осуществляются в сети Интернет, где отсутствует четкая идентификация участников, и, как следствие, данные операции проходят анонимно;

– распространенность данной виртуальной валюты позволяет осуществлять трансграничные транзакции любого объема и вне зависимости от времени суток; – децентрализованный характер криптовалюты делает ее неподконтрольной государственным органам и финансовым учреждениям;

– осуществляемые транзакции протекают с высокой скоростью, и, как следствие, перехватить и заблокировать такие операции практически невозможно;

– операции не требуют проверок, что позволяет сделать их необратимыми;

– отсутствие законодательной базы в сфере обращения виртуальных валют делает их свободными во многих странах;

– возможность конвертации позволяет осуществлять обмен фиатных денежных средств1 на криптовалюту и наоборот;

– транснациональный характер позволяет обмениваться криптовалютой за пределами страны;

– существование сервисов, которые позволяют пользователям скрывать происхождение и назначение транзакций при осуществлении операций с криптовалютой;

– открытый код позволяет добывать виртуальные монеты любому желающему, то есть каждый человек может осуществлять деятельность, связанную с майнингом[1].

В свою очередь отсутствие четкого нормативно-правового регулирования криптовалют на международном уровне осложняет борьбу с их криминальным использованием, а возможность использования анонимизирующих сервисов и VPN дополнительно затрудняет идентификацию участников незаконных транзакций.

Значительная часть операций с криптовалютами связана с незаконной деятельностью, и эта тенденция усиливается при

[1] Лукошина П.А. Механизмы финансирования экстремистской и террористической деятельности с использованием криптовалюты // Вестник Уральского юридического института МВД России. 2024. № 1(41). С. 121–124.

недостаточной технологической оснащенности правоохранительных органов.

Применение криптовалюты в экстремистских преступлениях усложняет работу следственных органов, требуя новых правовых инструментов и подходов к анализу информации о преступлениях.

В настоящее время внедрение современных технологий мониторинга блокчейн-транзакций, развитие нормативно-правовой базы и международного сотрудничества рассматриваются как ключевые направления борьбы с использованием криптовалют киберэкстремистами[1].

В целях выявления и последующей правильной уголовно-правовой оценки деятельности киберэкстремистов применяются следующие методы мониторинга и анализа блокчейн-транзакций для повышения кибербезопасности:

1) Использование специализированного программного обеспечения для анализа блокчейна, которое позволяет отслеживать цепочки перемещений цифровых активов, выявлять подозрительные кошельки и анализировать поведение участников рынка;

2) Ведутся базы данных адресов, связанных с противоправной деятельностью, что помогает в идентификации и деанонимизации подозреваемых;

3) Применяются методы кластеризации для выявления групп связанных адресов, даже если они на первый взгляд не связаны друг с другом;

4) Визуализация графов транзакций, которая помогает вручную исследовать сложные схемы переводов и находить аномалии;

5) Отслеживаются кошельки с крупными объемами средств и резкие перемещения активов, что может указывать на подготовку или проведение противоправных операций;

6) Сравниваются данные о транзакциях на разных биржах, анализируется активность портфелей, используются открытые блокчейн-обозреватели (Etherscan, Solscan) и сервисы оповещений (Whale Alert);

7) Используются алгоритмы для присвоения транзакциям и адресам оценок риска, что помогает выявлять потенциально опасные

[1] Парамонов А.В. Уголовно-правовые аспекты противодействия экстремизму в виртуальном пространстве // Актуальные проблемы государства и права. 2020. Т. 4, № 13. С. 141–150.

операции и предотвращать отмывание денег и финансирование терроризма;

8) Современные системы анализа используют ИИ и машинное обучение для выявления паттернов поведения, аномалий и автоматического формирования гипотез о противоправной деятельности;

9) Для деанонимизации участников могут использоваться пылевые атаки (dusting attack), когда на кошелек отправляется небольшая сумма с целью отслеживания дальнейших транзакций и связи с другими адресами;

10) Использование приватных блокчейнов позволяет контролировать все узлы сети, быстро реагировать на угрозы и исключать ряд атак, характерных для публичных сетей.

Эти методы позволяют правоохранительных органам не только отслеживать и анализировать транзакции в блокчейне, но и выявлять преступные схемы, предотвращать финансирование терроризма и обеспечивать кибербезопасность на национальном уровне.

Список источников

1. Баранов В.В. Некоторые аспекты противодействия финансированию экстремизма в условиях цифровой трансформации общества // Право и государство: теория и практика. 2023. № 10(226). С. 217–219.

2. Парамонов А.В. Уголовно-правовые аспекты противодействия экстремизму в виртуальном пространстве / А.В. Парамонов, В.В. Харин // Актуальные проблемы государства и права. 2020. Т. 4, № 13. С. 141–150.

3. Лукошина П.А. Механизмы финансирования экстремистской и террористической деятельности с использованием криптовалюты // Вестник Уральского юридического института МВД России. 2024. № 1(41).

Е.Н. Яковец
Российская таможенная академия

О некоторых проблемах борьбы с экстремистской опасностью в киберпространстве

Аннотация. В статье рассматривается понятие киберэкстремизма. Анализируется его тесная взаимосвязь с кибертерроризмом. Говорится об актуальных на сегодняшний день угрозах, связанных с использованием экстремистами виртуального пространства. Прослеживается взаимосвязь киберэкстремизма с информационными атаками, предпринимаемыми коллективным Западом. Ставится вопрос о необходимости возрождения в России микроэлектронной индустрии, а также об установлении на международном уровне контроля за кибероружием.

Ключевые слова: киберэкстремизм; кибертерроризм; неконтролируемая миграция; государственный кибертерроризм; кибероружие; технологическая независимость.

В условиях развития научно-технического прогресса информационные технологии и компьютерные сети всё активнее используют экстремистские организации с целью создания хаоса как внутри отдельных стран, так и на мировой арене. В виртуальном пространстве ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение в свои ряды новых членов, осуществление незаконных финансовых операций и т.д. Всё это позволяет говорить о появлении ещё одной опасной разновидности компьютерной преступности – киберэкстремизма. В современной юридической науке обобщённое определение данного криминального явления отсутствует. Систематизация различных точек зрения на этот счёт приводит к выводу о том, что киберэкстремизм – это экстремизм в киберпространстве. Он рассматривается как приверженность к крайним взглядам и мерам. Среди таких мер можно отметить провокацию беспорядков, террористических акций, методов нелегального противодействия

властям и др.[1] Комплекс подобных преднамеренных преступных деяний в киберпространстве создаёт угрозу безопасности личности, общества и государства. Они тесно связаны с терроризмом, являясь его питательной средой, и могут сопровождаться насилием или угрозой применения насилия, – с целью оказания психологического воздействия на сознание людей в политических, социальных, религиозных или идеологических целях.

Существенным фактором, способствующим дестабилизации обстановки в России, является волна миграции из южных республик бывшего СССР. Потоки мигрантов, в том числе прибывающих в Россию нелегально, в арифметической (если не геометрической) прогрессии захватывают практически все регионы России[2]. Не проявляя никакого интереса к интеграции в российское общество, мигранты, среди которых немало приверженцев радикальных исламских движений, объединяются в национальные диаспоры, устанавливая в этнических анклавах свои порядки, навязывая коренным россиянам новые правила поведения и дресс-кода[3]. Председатель Национального антикоррупционного комитета, член Совета по правом человека при Президенте РФ К.В. Кабанов, комментируя результаты опроса среди мигрантов-граждан Средней Азии, обращает внимание на то, что на вопрос: «Готовы ли вы с оружием в руках отстаивать свои национальные, культурные и религиозные ценности на территории Российской Федерации?», 40% из них отвечают: «Да»[4]. Показательно, что новоиспечённые граждане

---

[1] Панталеева Н.С., Пархитько Н.П. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. 2019. № 3. С. 47.

[2] Сошенко А. В Москве славян уже меньше половины. При такой миграционной политике скоро по всей России будет, как в столице // Русская народная линия. Православие. Самодержавие. Народность. Информационно-аналитическая служба. 2021. 30 августа URL: https://ruskline.ru/news_rl/2021/08/30/ v_moskve_ slavyan_uzhe_menshe_poloviny_(дата обращения: 14.02.2025).

[3] Иванов А. Таджикистан направил в РФ пять инспекционных поездок для проверки условий жизни мигрантов // Завтра. 2023. 13 августа. URL: https://zavtra.ru/events/tadzhikistan_napravil_v_rf_pyat_inspektcionnih_komissij_dlya_proverki_uslovij_zhizni_migrantov (дата обращения: 03.01.2025).

[4] Кукова А. Глава НАК Кабанов сравнил приезд мигрантов с «тихим захватом» России // MK.RU 2022. 19 октября URL: www.mk.ru/politics/2022/10/19/glava-nak-kabanov-sravnil-priezd-migrantov-s-tikhim-zakhvatom-rossii.html (дата обращения: 03.01.2025).

России – выходцы из среднеазиатских стран, получая паспорт, не спешат становиться на воинский учёт, зато сразу же занимают очередь на приобретение огнестрельного оружия. Со временем у мигрантов и их потомков появятся формальные и неформальные структуры, возглавляемые влиятельными лидерами, они будут просачиваться в муниципальные и государственные органы, в том числе – силовые ведомства[1].

Для продвижения своих целей миграционная среда активно использует информационные технологии, посредством которых она рекрутирует в свои ряды новых сторонников, настраивает соплеменников на противодействие законным требованиям органов правопорядка, устанавливает межрегиональные и международные связи с национал-радикалами. Владельцы подобных сайтов понимают, что их деятельность противозаконна, и стараются скрывать подобные сайты в «даркнете» или размещать их на зарубежных серверах[2] Особую остроту данная проблема обретает именно сегодня, когда страна находится в конфронтации практически со всем западным миром, который, по мнению многих аналитиков, и стоит у истоков данных деструктивных процессов.

Развивая эту мысль, следует отметить, что информационные технологии могут использоваться не только экстремистами или террористами внутри отдельно взятой страны, но и представителями силовых структур развитых в кибернетическом отношении стран в ходе ведения так называемых «гибридных войн»[3]. Англосаксы

---

[1] Иванов А. Новые граждане РФ (уроженцы Средней Азии) массово вооружаются // Завтра. 2023. 18 марта. URL: https://zavtra.ru/events/novie_grazhdane_rf_(vihodtci_iz_srednej_azii)_massovo_vooruzhayutsya (дата обращения: 15.02.2025).

[2] Клименский М.М. Кибертерроризм как социально-политическое явление: отличительные признаки и основные причины активизации на современном этапе // Внешнеполитические интересы России: история и современность: сборник материалов Всероссийской научной конференции, приуроченной к 100-летию начала Первой мировой войны / Ответственный редактор А.Н. Сквозников / Самарская гуманитарная академия; Самарский государственный университет. Самара, 2014. С. 84–90.

[3] Третья мировая на пороге. Какая она?: интервью генерал-полковника, специалиста в области геополитики, конфликтологии, международных отношений и военной истории, президента Академии геополитических проблем Л.Г. Ивашова главному редактору газеты «Аргументов недели» А. Угланову // Аргументы недели. № 5 (749). 2021. 10–16 февраля. С. 6.

совместно с другими странами НАТО, примеряя на себя «тогу миротворцев», активно продвигают возможность использования виртуального пространства для осуществления информационных атак с использованием сил, средств и методов, заимствованных у киберэкстремистов и кибертеррористов. Причём, врагом номер один для них в этом плане является Россия[1]. После начала Российской Федерацией специальной военной операции на территории Украины Запад совместно с «самостийниками» стали практиковать продвижение своих радикальных экстремистских идей, направленных на дискредитацию руководства России и проводимой им политики. Признавая, что победить Россию на поле боя не удаётся, наши враги стремятся развалить её изнутри. Используется в этом плане и экстремистская миграционная среда, внутри которой вербуются исполнители наиболее кровавых и резонансных террористических актов.

Как справедливо отмечал в своё время профессор О.В. Дамаскин, «кое-где информационный терроризм и экстремизм стали элементами государственной политики. В некоторых странах активно ведутся работы над компьютерными программами, являющимися информационным оружием. Причём объектами для такого оружия всё чаще становятся отдельные личности, социальные группы, принимающие решения, а не только массы и государственные структуры, как это было не так давно. Иными словами, избирательность этого оружия растёт, именно люди, в первую очередь высокопоставленные, являются теперь главной целью в информационных войнах, и их принуждают к выбору необходимых противнику решений. Информационное воздействие на государство, общество, отдельно взятого человека, в конечном счёте, оказывается более эффективным и экономичным, чем политическое, экономическое и даже силовое, военное»[2].

Таким образом, в последнее время на международном уровне наблюдается переход конкуренции в киберпространстве (как, впрочем, и в реальном мире) на качественно новый уровень: теперь это противоборство, предполагающее нанесение потенциальному

---

[1] Кто главный враг Запада: Россия или терроризм? // ОБЗОР.PRESS. Переводы иностранной прессы. 2016. 23 марта. URL: https://obzor.press/press/18386-kto-glavnyij-vrag-zapada-rossiya-ili-terrorizm (дата обращения: 17.02.2025).

[2] Дамаскин О.В. Россия в современном мире: проблемы национальной безопасности: Монография. М.: Флинта; Наука, 2007. С. 267.

противнику ощутимого ущерба посредством применения кибероружия. Это влечёт за собой существенное повышение уровня международной конфронтации, приводит к стиранию грани между войной и миром в условиях, когда не имеется никаких регуляторных договорённостей между странами, а в Военной доктрине РФ, как и у её оппонентов, содержатся положения, гарантирующие нанесение ответных ударов по агрессорам[1].

Существенной проблемой в этой сфере для России является её технологическая зависимость от зарубежных разработчиков компьютерной техники и программного обеспечения. Не случайно поэтому, что в качестве приоритетных направлений научно-технических разработок в области борьбы с экстремистской и террористической угрозой *Концепция противодействия терроризму в Российской Федерации,* утверждённая Президентом РФ 5 октября 2009 г.[2], называет создание и внедрение эффективных средств систем связи, отвечающих требованиям защищённости от компьютерных атак (п. 37, пп. «в»).

Таким образом, в условиях обострения межгосударственных отношений, разрушения системы однополярного мира, возвращения на мировую арену России и появления новой сверхдержавы – Китая, кибероружие становится действенным инструментом глобального противостояния. От того, кто быстрее сможет освоить передовые цифровые технологии, создать мощную систему защиты от киберэкстремизма и кибертерроризма, зависит не только национальная безопасность той или иной страны, но и в целом мировой порядок.

Кроме того, само по себе применение кибероружия в силу его колоссального разрушительного потенциала необходимо поставить под международный контроль и приравнять его к использованию иных видов оружия массового поражения.

---

[1] См.: Военная доктрина Российской Федерации (утв. Президентом РФ 25 декабря 2014 г. № Пр-2976). П. 21, пп. «у» // Российская газета. 2014. 30 декабря.
[2] Российская газета. 2009. 20 октября.

Список источников

4. Военная доктрина Российской Федерации (утв. Президентом РФ 25 декабря 2014 г. № Пр-2976). П. 21, пп. «у» // Российская газета. 2014. 30 декабря.

5. Дамаскин О.В. Россия в современном мире: проблемы национальной безопасности: Монография. М.: Флинта; Наука, 2007. 428 с.

6. Клименский М.М. Кибертерроризм как социально-политическое явление: отличительные признаки и основные причины активизации на современном этапе // Внешнеполитические интересы России: история и современность: сборник материалов Всероссийской научной конференции, приуроченной к 100-летию начала Первой мировой войны / Ответственный редактор А.Н. Сквозников; Самарская гуманитарная академия; Самарский государственный университет. Самара, 2014. С. 84–90.

7. Панталеева Н.С., Пархитько Н.П. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. 2019. № 3. С. 47–52.

Сведения об авторах

Бардачевский Руслан Игоревич – инспектор контрольно-следственного управления Главного следственного управления Следственного комитета Российской Федерации, подполковник юстиции, кандидат юридических наук.

Боков Сергей Никанорович – доцент кафедры криминалистики юридического факультета ФГБОУ ВО «Воронежский государственный университет», кандидат медицинских наук, доцент.

Бражников Дмитрий Анатольевич – доцент кафедры оперативно-разыскной деятельности Российской таможенной академии кандидат юридических наук, доцент.

Быкова Елена Георгиевна – доцент кафедры уголовного права, криминологии и уголовного процесса Екатеринбургского филиала Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции

Бычкова Екатерина Игоревна – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

Васюков Виталий Федорович – доктор юридических наук, профессор, главный научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева. 125080, Российская Федерация, г. Москва, ул. Врубеля, 12.

Вахмянина Наталья Борисовна – директор Екатеринбургского филиала Московской академии Следственного комитета имения А.Я. Сухарева, кандидат юридических наук, доцент.

Галдин Максим Владимирович – доцент кафедры уголовного права, криминологии и уголовного процесса Новосибирского филиала ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева», полковник юстиции.

Галкин Денис Викторович – заведующий кафедрой криминалистики Хабаровского филиала ФГКОУ ВО «Московская академия Следственного комитета Российской

Федерации имени А.Я. Сухарева», кандидат юридических наук, доцент, полковник юстиции.

Земскова Елена Николаевна – преподаватель кафедры криминалистики Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, полковник юстиции.

Зуев Сергей Васильевич – профессор кафедры судебной и правоохранительной деятельности Южно-Уральского государственного университета (национального исследовательского университета), доктор юридических наук, профессор.

Кожевников Иван Николаевич – адвокат адвокатского бюро «Ри-консалтинг» г. Моска, соискатель.

Колычева Алла Николаевна – старший преподаватель кафедры криминалистики и предварительного расследования в ОВД. Орловский юридический институт МВД России имени В.В. Лукьянова, кандидат юридических наук.

Карагодин Валерий Николаевич – заведующий кафедрой криминалистики Екатеринбургского филиала ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева», заслуженный юрист РФ, доктор юридических наук, профессор.

Лебедева Анна Андреевна – доцент кафедры криминалистика Московской академии следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Литвишко Петр Андреевич – начальник управления правовой помощи и правоохранительного содействия Главного управления международно-правового сотрудничества Генеральной прокуратуры Российской Федерации, кандидат юридических наук, Почетный работник прокуратуры Российской Федерации, Почетный работник Следственного комитета при прокуратуре Российской Федерации, государственный советник юстиции 3 класса, полковник юстиции.

Озеров Кирилл Игоревич – доцент кафедры уголовного права и криминологии факультета права и психологии Межрегионального открытого социального института, кандидат юридических наук.

Озеров Игорь Николаевич – заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета имени А.Я Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Османова Надежда Валерьевна – декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета, кандидат юридических наук, доцент.

Прорвич Владимир Антонович – профессор-исследователь Департамента уголовного права, процесса и криминалистики Национального исследовательского университета «Высшая школа экономики», доктор юридических наук, доктор технических наук, профессор, Почетный профессор Московской академии Следственного комитета России.

Пшеничнов Илья Михайлович – старший преподаватель кафедры уголовного права, криминологии и уголовного процесса Нижегородского филиала Санкт-Петербургской академии Следственного комитета, кандидат юридических наук, майор юстиции.

Решетихин Вадим Викторович – курсант 1 курса магистратуры факультета подготовки криминалистов ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации». (Научный руководитель – Летёлкин Н.В., доцент кафедры криминалистики Нижегородского филиала ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», кандидат юридических наук, доцент, подполковник юстиции).

Саркисян Армен Жораевич – декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, подполковник юстиции, кандидат юридических наук, доцент.

Стояновский Максим Валериевич – доцент кафедры криминалистики юридического факультета ФГБОУ ВО «Воронежский государственный университет», кандидат юридических наук, доцент.

Шашков Владимир Михайлович – старший инспектор третьего следственного управления Главного следственного управления Следственного комитета Российской Федерации, подполковник юстиции.

Яковец Евгений Николаевич – профессор кафедры уголовно-правовых дисциплин Российской таможенной академии, Заслуженный юрист РФ, доктор юридических наук, профессор.

Оглавление

НАУЧНЫЕ ОСНОВЫ ГОСУДАРСТВЕННОЙ ПРОГРАММЫ БОРЬБЫ С КИБЕРЭКСТРЕМИЗМОМ

Всероссийский круглый стол, посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова

Москва, 4 апреля 2025 г.

Подписано в печать: 26.09.2025
Формат 60x90 1/16
Усл. печ. л. 9,8
Тираж 100 экз.
Компьютерная верстка,
техн. редактирование – А.Ж. Саркисян, И.Д. Нестерова
Заказ № 525

Отпечатано в типографии Московской академии Следственного комитета имени А.Я. Сухарева,
ул. Врубеля, д. 12