ISSN 2500-1442

Научная статья
УДК 343.85:004
EDN ZCLJNS
DOI 10.17150/2500-4255.2024.18(1).89-95

ЦИФРОВОЕ ПРОСТРАНСТВО КАК МЕСТО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

В.О. Давыдов
Тульский государственный университет, г. Тула, Российская Федерация

Информация о статье

Дата поступления
15 января 2024 г.

Дата принятия в печать
28 февраля 2024 г.

Дата онлайн-размещения
22 марта 2024 г.

Ключевые слова

Экстремизм; цифровое пространство; компьютерное устройство; цифровой след; информационно-телекоммуникационная сеть; криминалистически значимая информация; преступные действия; контент; место совершения преступления

Аннотация. Инновации цифровой коммуникации детерминировали тенденцию устойчивой причинно-следственной связи между разнообразием технологий и качественными изменениями механизма преступлений экстремистской направленности. По сути, в обстановке развития процессов глобальной информатизации произошла смена парадигмы — способы трансформации социального поведения, основанные на цифровой коммуникации и технологиях социальной инженерии, стали одним из узловых элементов в механизме воздействия на сознание объектов экстремистской индоктринации. В связи с этим представляется необходимым научное осмысление с позиций криминалистики определения цифрового пространства как места совершения преступления экстремистской направленности с целью дальнейшей выработки рекомендаций по выявлению, фиксации и систематизации доказательственной и иной криминалистически значимой информации, формирования криминалистической характеристики и познания на ее основе механизма преступного деяния подобного вида. Методологическую основу научного исследования составил всеобщий диалектический метод научного познания. Кроме того, в ходе исследования применялись следующие общенаучные и частнонаучные методы: системно-структурный, формально-логический, статистический, конкретно-социологический, анализ и синтез, индукция и дедукция, аналогия. Также осуществлялось обобщение данных, моделирование. По мнению автора, для понимания механизма следообразования в цифровой среде необходимо определить изменения, произошедшие в результате электромагнитных взаимодействий сигнала и среды, в которой происходила обработка сигнала, а также выяснить, какие факторы оказали влияние на процесс электромагнитных взаимодействий. Следовательно, чтобы выявить, зафиксировать и установить связь между цифровыми следами и электромагнитными взаимодействиями, необходимо установить перекрещивающуюся взаимосвязь между компьютерным устройством, элементом цифровой инфраструктуры, а также интересующим субъект расследования событием либо действием, оставившим свое отражение. В отношении преступлений экстремистской направленности, совершенных в цифровом пространстве, целесообразно толковать место совершения преступления как место непосредственного совершения основных преступных действий экстремистской направленности. По сути, это место ввода экстремистского контента и выхода в информационно-телекоммуникационную сеть цифрового пространства с последующей реализацией из этого места преступного деяния экстремисткой направленности, независимо от места, где наступили последствия.

Original article

DIGITAL SPACE AS A SCENE OF EXTREMIST CRIMES

Vladimir O. Davydov
Tula State University, Tula, the Russian Federation

Article info

Received
2024 January 15

Accepted
2024 February 28

Available online
2024 March 22

Abstract. Innovations in digital communications determined a trend for a sustainable causal link between technological diversity and qualitative changes in the mechanism of extremist crimes. Essentially, the processes of global informatization led to a paradigm shift, and the methods of transforming social behavior based on digital communications and social engineering technologies became some of the key elements in influencing the minds of the objects of extremist indoctrination. Due to this, it is necessary to offer a forensically grounded definition of digital space as a scene where extremist crimes are committed with the purpose of developing recommen-

ISSN 2500-1442

Keywords

Extremism; digital space; a computer device; digital footprint; information and telecommunication network; forensically relevant information; criminal acts; content; the scene of the crime

dation for identifying, capturing and systematizing evidentiary and other forensically relevant information, developing a forensic characteristic and then using it to understand the mechanism of suchlike criminal acts. The methodological basis for the research is the general dialectic method of research cognition. Besides, some general and special research methods were used: systemic-structural, formal-logical, statistical, specific-sociological, analysis and synthesis, induction and deduction, analogy. Data consolidation and modelling were also carried out. According to the author, in order to understand the mechanism of trace formation in the digital environment, it is necessary to identify changes resulting from the electromagnetic interactions between the signal and the environment in which the signal was processed, and to understand what factors influenced the process of electromagnetic interactions. Consequently, in order to identify, capture and establish a link between digital traces and electromagnetic interactions, it is necessary to establish a crossover mutual relationship between a computer device, a digital infrastructure element, as well as an event of interest to the subject of the investigation or an action that has left its reflection. For the extremist crimes committed in the digital space, it is expedient that the crime scene should be interpreted as the place where key criminal extremist actions were committed. Essentially, it is the place where extremist content was uploaded, the information and telecommunication network of the digital space was entered, and the criminal action of extremist nature was then committed, regardless of the place where its consequences happened.

Агрессивное поведение сопровождает социум с момента его зарождения. Но если на ранних стадиях развития человеческой общности агрессия в определенной степени была детерминирована рядом эволюционных причин, то на последующих этапах она породила значительное количество проблем как регионального, так и мирового характера.

Среди многочисленных форм проявления агрессии в XXI в. особое место в силу масштабности и разрушительности своих проявлений занимает экстремистская деятельность. С конца прошлого столетия облик экстремизма интенсивно меняется, а сфера противоправной деятельности подобной направленности неуклонно трансформируется в территориальном, мотивационном, технологическом и иных аспектах, превращая его в деструктивную силу, угрожающую национальной безопасности любого из государств мирового сообщества.

Как следствие, в ряде нормативных правовых актов, принятых в последние годы в Российской Федерации, констатировано возникновение новых проблем борьбы с преступлениями экстремистской направленности из-за сложных процессов социально-экономического развития в условиях перехода к информационному обществу[1].

Бесспорно, глобальная цифровизация социума, обусловленная активным развитием цифровых технологий и средств коммуникации, привела к беспрецедентному расширению возможностей доступа к самому разнообразному спектру информационных ресурсов. Свободное доведение и потребление информации способствует усилению социальной активности индивидов, служа созидательным целям повышения эффективности институтов публичного управления.

Однако очевиден и тот факт, что любой прогресс имеет свою обратную, негативную сторону. Еще великий русский мыслитель Лев Николаевич Толстой отмечал, что «прогресс одной стороны человеческой жизни повсеместно выступает регрессом другой ее стороны» [1, с. 78]. Так и инновации цифровой коммуникации, с одной стороны, детерминировали тенденцию достаточно устойчивой причинно-следственной связи между разнообразием технологий, а с другой — привели к качественным изменениям механизма экстремистской деятельности.

Повышенный интерес лидеров экстремистских формирований к цифровому пространству не случаен. Уникальность последнего состоит в том, что оно не находится в ведении отдельного государства, конкретного юридического или физического лица. Более того, в нем еще недостаточно эффективен контроль за содер-

[1] См. например: Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года : указ Президента Российской Федерации от 29 мая 2020 г. № 344 // Собрание законодательства Российской Федерации. 2020. № 22. Ст. 3475 ; О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Там же. 2021. № 27 (часть II). Ст. 5351 ; Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей : указ Президента Российской Федерации от 9 нояб. 2022 г. № 809 // Там же. 2022. № 46. Ст. 7977.

жательной направленностью информационного контента, что открывает, по сути, достаточно широкие возможности для распространения экстремистской идеологии и вовлечения в деструктивную деятельность все новых и новых «рекрутов» [2, с. 56].

Результаты анализа официальных данных правоохранительной статистики приводят к выводу о наличии тенденции увеличения количества преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий: так, если в 2019 г. было зарегистрировано 257 деяний данного вида, то в 2020 г. — 340, в 2021 г — 455, в 2022 г. — 493. По итогам 2023 г., несмотря на снижение числа выявленных фактов публичных призывов к осуществлению экстремистской деятельности (ст. 280 УК РФ) на 25,6 % (367 деяний), на 11,8 % увеличилось количество преступлений, связанных с публичными призывами к осуществлению террористической деятельности, с публичным оправданием терроризма или пропагандой терроризма (ст. 205.2 УК РФ) — 548 деяний[2].

Заметим, что данному обстоятельству в немалой степени способствуют закономерности двойственной социально-технологической природы цифрового пространства, а также наличие у цифровых технологий определенного криминально привлекательного функционала.

В числе последнего, имеющего, на наш взгляд, значение в аспекте криминалистического обеспечения процесса расследования, следует выделить:

1. Анонимность доступа к цифровой среде и масштабную аудиторию ее пользователей, обеспечиваемую использованием разнообразных способов сокрытия идентификационной информации (например, технологии IP-телефонии и подмены идентификационных телефонных номеров посредством SIP-телефонии, сквозное шифрование, отсылка к web-зеркалам интернет-платформ и др.).

2. Трансграничный характер преступной деятельности, при котором субъект деструктивной активности, объект посягательства и жертва (а в качестве последней в рассматриваемом случае может выступать неограниченный круг лиц), как правило, находятся под юрисдикцией различных государств.

3. Высокую скорость распространения, мультимедийность деструктивного контента и возможность одновременного воздействия на различные модальности восприятия потенциальной аудитории за счет креолизованности информационных объектов.

Полагаем, что в обстановке развития процессов глобальной информатизации произошла смена парадигмы — способы трансформации социального поведения, основанные на цифровой коммуникации и технологиях социальной инженерии, стали одним из узловых элементов в механизме воздействия на сознание объектов экстремистской индоктринации [3, с. 62].

В сложившихся условиях практика расследования преступных деяний экстремистской направленности, совершаемых в цифровом пространстве, пытается самостоятельно реагировать на возникающие проблемы правового, организационного, научно-технического, информационного и методического обеспечения, нарабатывая опыт их разрешения применительно к современным условиям деятельности правоохранительных органов. Однако подобный опыт не обеспечивает в должной степени специалистов-практиков необходимым объемом знаний о расследуемой преступной деятельности и рекомендациями по ведению работы в тех или иных следственных ситуациях.

В связи с этим представляется необходимым научное осмысление с позиций криминалистики определения цифрового пространства как места совершения преступления экстремистской направленности с целью дальнейшей выработки рекомендаций по выявлению, фиксации и систематизации доказательственной и иной криминалистически значимой информации, формирования криминалистической характеристики и познания на ее основе механизма преступного деяния подобного вида.

Думается, что это возможно путем обращения к понятию цифрового пространства, общему понятию «место совершения преступления», разрабатываемому в криминалистике, и рассмотрению особенностей применения выработанных положений относительно цифрового пространства.

Исходя из основополагающих положений теории познания, любое событие преступного деяния (и преступления экстремистской направленности, совершенные в цифровом пространстве, безусловно, не являются исключением) как одно из материальных явлений действи-

[2] Состояние преступности в Российской Федерации // Официальный портал МВД России. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics.

тельности обладает свойством отражения своих специфических черт в окружающей среде в виде различного рода следов-последствий. Следовательно, любому преступлению присуща такая неотъемлемая ключевая характеристика, как место совершения, которое в совокупности со временем совершения образует его пространственно-временные координаты [4, с. 9].

При этом, как справедливо указывают профессора А.Ф. Волынский и В.П. Лавров, реальные процессы отражения сопряжены с взаимодействием объектов материального мира. Подобное взаимодействие представляет собой процесс взаимного обмена энергией и веществом, в результате чего происходит отображение не только формы взаимодействующих объектов, но и их частиц, особенностей энергии, а, по сути, информации в самом широком понимании этого слова [5, с. 39].

Полагаем, что цифровое пространство, являющееся, по существу, искусственно созданной частью окружающей среды, следует определять как элемент информационного пространства, интегрирующий цифровые процессы, средства цифрового взаимодействия, совокупность цифровых инфраструктур, а также информационные ресурсы. Данное понимание позволяет охватывать всевозможные противоправные деяния, в том числе и экстремистской направленности, совершаемые с использованием средств цифрового взаимодействия, различных информационно-телекоммуникационных технологий и компьютерных устройств[3].

Очевидно, что цифровое пространство не имеет территориальных границ, а место совершения деяния экстремистской направленности и место наступления последствий, обусловленных таким деянием, могут, во-первых, находиться на большом расстоянии друг от друга, а, во-вторых, причинять вред неограниченному кругу лиц, что, в свою очередь, порождает определенные трудности в установлении места совершения преступления.

Не вызывает сомнений и тот факт, что сама потребность в определении места совершения преступления в процессе раскрытия и расследования последнего продиктована как материальным и процессуальным законодательством, так и соответствующими криминалистическими рекомендациями.

В то же время дефиниция рассматриваемой категории по-прежнему относится к числу дискуссионных вопросов вследствие отсутствия в российском законодательстве прямого указания на то, что следует понимать под понятием «место совершения преступления». Так, применительно к вопросу пространственного действия уголовного закона возникают такие трактовки:

– это место совершения противоправного деяния;

– это место наступления общественно-опасных последствий;

– это место, где находится исполнитель преступления [6, с. 156].

В свою очередь, практические работники достаточно часто руководствуются правилом «Forum delicti commissi», обосновывающим определение территориальной подсудности исходя из места совершения деликта.

С позиций отечественной криминалистики под местом совершения преступления принято понимать место совершения основных преступных действий в процессе этапов осуществления единого преступного умысла, а также место окончания преступления [7–9].

Думается, что подобный подход в аспекте преступлений экстремистской направленности, совершенных в цифровом пространстве, нуждается в определенном уточнении. И причин тому, на наш взгляд, несколько.

Во-первых, преступления рассматриваемого вида неизменно связаны с образованием особых цифровых следов[4] в программной сфере используемых средств цифрового взаимодействия и цифровых инфраструктур. При этом подобные следы, как справедливо указывает В.А. Мещеряков, в силу своей природы не обладают всей совокупностью характерных осо-

[3] В настоящем исследовании под категорией «компьютерное устройство» предлагается понимать не только стационарный персональный компьютер в его традиционном виде (ПЭВМ), но и другие технические устройства, функционирующие на основе процессора и специальных программных алгоритмов, позволяющие осуществлять доступ к информационно-телекоммуникационным ресурсам сети Интернет, и локальных компьютерных сетей.

[4] Под категорией «цифровой след» нами предлагается понимать совокупность сведений (данных, сообщений), образующих криминалистически значимую информацию о событиях и действиях, отраженную в искусственно созданной материальной среде — цифровом пространстве, выраженную посредством электрических сигналов в форме, пригодной для обработки с использованием компьютерных устройств, в результате создания либо модификации определенного кода на электронном носителе компьютерного устройства.

бенностей «традиционных» материальных или идеальных следов [10, с. 426].

Во-вторых, сам объективный характер цифровых следов, в понимании следов материальных, тоже отличен ввиду наличия в них определенной доли субъективной природы: они зависят от способов считывания и не имеют жесткой связи с устройством, осуществившим запись информации, что, в свою очередь, ведет к тому, что содержащаяся в них криминалистически значимая информация проще поддается фальсификации или повреждению вследствие ошибок считывания, записи или переформатирования.

Например, на практике при изменении системного времени компьютерного устройства, время, регистрируемое файлами при их создании либо изменении, будет соответствовать не реальному временному промежутку, а тому, который указан в системе и, соответственно, был изменен. Как следствие, при фиксации временных характеристик цифрового следа необходимо учитывать возможность изменения пользователем системного времени компьютерного устройства, что может привести к сложностям в определении временных характеристик исследуемой криминалистически значимой информации.

В-третьих, не представляется возможным и отнесение цифровых следов к следам идеальным ввиду того обстоятельства, что носителем идеальных следов может быть только человек.

Общепризнано, что основой же механизма образования цифровых следов является их электронно-цифровое отображение, происходящее в искусственно созданных материальных средах цифрового пространства: памяти электронных носителей информации средств цифрового взаимодействия, каналах цифровых инфраструктур передачи информации, объединяющих, в том числе, и информационно-телекоммуникационные сети и информационные ресурсы [11–14].

Сам же след в данном случае, на наш взгляд, будет представлять собой сложную информационную структуру, способную содержать в себе как цифровые значения параметров объектов, так и иную вспомогательную информацию, определяющую его принадлежность к конкретной из названных сред.

Очевидно и то, что для понимания механизма следообразования в цифровой среде необходимо определить изменения, произошедшие в результате электромагнитных взаимодействий сигнала и среды, в которой происходила обработка сигнала, а также то, какие факторы оказали влияние на данный процесс электромагнитных взаимодействий.

Следовательно, чтобы выявить, зафиксировать и установить связь между цифровыми следами и электромагнитными взаимодействиями, необходимо установить перекрещивающуюся взаимосвязь между компьютерным устройством, элементом цифровой инфраструктуры (например, информационно-телекоммуникационной сетью[5]), а также интересующим субъект расследования событием либо действием, оставившим свое отражение.

Полагаем, что применительно к указанной ситуации в порядке научной дискуссии можно предложить следующие возможные варианты места совершения преступления экстремистской направленности в цифровом пространстве:

– местоположение DNS-сервера как программного компонента вычислительной системы, выполняющего сервисные функции по запросу пользователя, предоставляющего ему доступ к определенным ресурсам или услугам;

– местоположение потерпевшего;

– место совершения основных преступных действий экстремистской направленности в процессе этапов осуществления единого преступного умысла.

Подвергнем предложенные варианты краткому анализу.

На первый взгляд наиболее логичным представляется определение места совершения преступления по месту, где физически расположено компьютерное устройство — DNS-сервер, осуществляющее две основные функции, значимые в аспекте поиска и фиксации доказательственной информации, а именно — хранение данных о соответствии имени домена конкретному IP-адресу и кэшировании ресурсных записей прочих DNS-серверов. Однако масштабы каналов цифровых инфраструктур передачи информации, а также использование преступниками современных способов обеспечения анонимности доступа к цифровой среде, в том числе и в отношении сведений IP-адресов, делают поисково-познавательную деятельность субъекта расследования в подобном аспекте весьма неэффективной [15, с. 133].

[5] Под категорией «информационно-телекоммуникационная сеть» нами предлагается понимать технологическую систему, предназначенную для передачи информации по линиям связи, доступ к которой осуществляется с использованием компьютерного устройства.

Существенной особенностью преступлений экстремистской направленности, совершенных в цифровом пространстве, является и проблема определения личности потерпевшего. Согласимся с мнением М.А. Болвачева, что в рассматриваемом аспекте экстремистские материалы, как правило, носят обезличенный характер, направленный не на конкретного человека, но на расу, этнос, конфессию или социальную группу [16, с. 48]. Подобное обстоятельство в принципе исключает возможность определения конкретного потерпевшего.

Полагаем, что специфика совершения преступления в цифровом пространстве (и преступления экстремистской направленности не являются в этом случае исключением) приводит к изменению ситуационной модели преступного деяния: в рассматриваемом нами случае цифровое пространство в определенной степени выступает в роли места совершения преступления, средствами будут являться компьютерные устройства (объекты материального мира), используемые для доступа к ресурсам информационно-телекоммуникационных сетей, а также цифровые объекты, посредством которых осуществлялась преступная деятельность. На данное обстоятельство, в частности, указывают и А.Н. Колычева и В.Ф. Васюков [17, с. 12].

В то же время, будучи местом совершения преступления, цифровое пространство содержит значительное количество криминалистически значимой информации в виде цифровых следов, определить физическое местонахождение которых не представляется возможным и, по сути, не целесообразно (например, хранение информации на удаленных серверах позволяет также удаленно такую информацию получать).

Однако совершение преступлений экстремисткой направленности в цифровом пространстве, безусловно, связано с использованием архитектуры и функциональных возможностей последнего. В частности, сокрытие личности преступника-экстремиста происходит не только и не столько, например, в информационно-телекоммуникационной сети, сколько с непосредственным использованием дополнительных компьютерных устройств. Следовательно, инструментарий сети становится средством взаимодействия в логической цепочке «злоумышленник — жертва», благодаря чему оно может сохранить информацию о местонахождении компьютерных устройств злоумышленника.

Изложенное приводит к следующему выводу. В отношении преступлений экстремистской направленности, совершенных в цифровом пространстве, целесообразно толковать место совершения преступления как место, непосредственного совершения основных преступных действий экстремистской направленности. По сути, это место ввода экстремистского контента и выхода в информационно-телекоммуникационную сеть цифрового пространства с последующей реализацией из этого места преступного деяния экстремисткой направленности, независимо от места, где наступили последствия. Например, в случае распространения публичных призывов к осуществлению экстремистской деятельности — это территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего подобные призывы, независимо от места нахождения другого лица.

Думается, что дальнейшее изучение сущности механизма преступлений экстремистской направленности, совершаемых в цифровом пространстве, должно способствовать приданию целенаправленного характера деятельности правоприменителей в сфере поиска и анализа доказательственной информации, имеющейся в информационно-телекоммуникационных сетях, а также формированию обоснованных криминалистических рекомендаций по совершенствованию организации и тактики обнаружения, фиксации и изъятия цифровых следов. Обозначенные в статье аспекты преследует именно эту цель — инициировать научную дискуссию, которая, безусловно, приведет к пониманию существующих проблем и к поиску путей их эффективного разрешения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Толстой Л.Н. Полное собрание сочинений : в 90 т. Т. 8. Педагогические статьи (1860–1863 гг.) / Л.Н. Толстой. — Москва : Художественная литература, 1936. — 485 с.

2. Girard J. Criminalistics: Forensic Science, Crime and Terrorism / J. Girard. — Jones, Bartlett Publishers, 2011. — 520 p.

3. Давыдов В.О. Методика расследования транснациональной преступной деятельности экстремистского характера : монография / В.О. Давыдов. — Москва : Юрлитинформ, 2018. — 440 с. — EDN ZIEALB.

4. Давыдов В.О. Информация в деятельности по раскрытию и расследованию преступлений: теория, практика, инновации : монография / В.О. Давыдов. — Москва : Юрлитинформ, 2021. — 248 с. — EDN BBBBYH.

5. Криминалистика : учебник / под ред. А.Ф. Волынского, В.П. Лаврова. — Москва : Юнити-Дана ; Закон и право, 2013. — 943 с.

6. Иванова Л.В. Цифровое пространство как место совершения преступления в условиях глобальных ограничений / Л.В. Иванова, Г.В. Пережогина. — DOI 10.21684/2411-7897-2020-6-4-155-171. — EDN PLNNQW // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. — 2020. — Т. 6, № 4 (24). — С. 156–171.

7. Гаврилин Ю.В. Криминалистика в понятиях и терминах : учеб. пособие / Ю.В. Гаврилин, А.Ю. Головин, И.В. Тишутина. — Москва : Книжный мир, 2006. — 384 с. — EDN UNILYN.

8. Белкин Р.С. Курс криминалистики : учеб. пособие / Р.С. Белкин. — Москва : Юнити, 2001. — 837 с.

9. Баев О.Я. Производство следственных действий: криминалистический анализ УПК России, практика, рекомендации профессионалов / О.Я. Баев, Д.А. Солодов. — Москва : Эксмо, 2008. — 203 с.

10. Мещеряков В.А. Следы цифрового века / В.А. Мещеряков. — EDN IFBYGN // Вопросы экспертной практики. — 2019. — № 51. — С. 423–426.

11. Brian J. Network File System Forensic Analysis / J. Brian. — Addison-Wesley Professional, 2005. — 600 p.

12. Easttom C. Digital Forensics, Investigation and Response / C. Easttom. — Jones : Bartlett Learning, 2021. — 403 p.

13. Nelson B. Guide to Computer Forensics and Investigations / B. Nelson, C. Steuart, A. Phillips. — Course Technology, 2018. — 688 p.

14. Ham J. Network Forensics: Tracking Hackers through Cyberspace / J. Ham, S. Davidoff. — Pearson Education, 2012. — 576 p.

15. Godwin J. Computer Forensics: Principles and Practices / J. Godwin, R. Anzaldua, L. Volonino. — Prentice Hall PTR, 2006. — 552 p.

16. Болвачев М.А. Использование социальных сетей при расследовании преступлений экстремистской направленности : дис. … канд. юрид. наук : 12.00.12 / М.А. Болвачев. — Калининград, 2022. — 206 с.

17. Колычева А.Н. Расследование преступлений с использованием компьютерной информации из сети Интернет : учеб. пособие / А.Н. Колычева, В.Ф. Васюков ; под ред. А.Г. Волеводза. — Москва : Проспект, 2022. — 200 с.

REFERENCES

1. Tolstoi L.N. *Complete Works*. Moscow, Khudozhestvennaya Literatura Publ., 1936. Vol. 8. 485 p.

2. Girard J. *Criminalistics: Forensic Science, Crime and Terrorism*. Jones, Bartlett Publishers, 2011. 520 p.

3. Davydov V.O. *The Methodology of Investigating Transnational Criminal Activities of Extremist Nature.* Moscow, Yurlitinform Publ., 2018. 440 p. EDN: ZIEALB.

4. Davydov V.O. *Information in the Activities of Investigating and Solving Crimes: Theory, Practice, Innovations.* Moscow, Yurlitinform Publ., 2018. 440 p. EDN: BBBBYH.

5. Volynskii A.F., Lavrov V.P. (eds.). *Criminology*. Moscow, Yuniti-Dana ; Zakon i Pravo Publ., 2013. 943 p.

6. Ivanova L.V., Perezhogina G.V. The Digital Space as a Crime Scene under Global Constraints. *Vestnik Tyumenskogo gosudarstvennogo universiteta. Sotsial'no-ekonomicheskie i pravovye issledovaniya = Tyumen State University Herald. Social, Economic, and Law Research*, 2020, vol. 6, no. 4, pp. 156–171. (In Russian). EDN: PLNNQW. DOI: 10.21684/2411-7897-2020-6-4-155-171.

7. Gavrilin Yu.V., Golovin A.Yu., Tishutina I.V. *Criminalistics in Concepts and Terms.* Moscow, Knizhnyi mir Publ., 2006. 384 p. EDN: UNILYN.

8. Belkin R.S. *A Course in Criminalistics.* Moscow, Yuniti Publ., 2001. 837 p.

9. Baev O.Ya., Solodov D.A. *Investigative Activities: a Criminalistic Analysis of Russian Criminal Procedure Code, Practice, Recommendations of Professionals.* Moscow, Ehksmo Publ., 2008. 203 p.

10. Meshcheryakov V.A. Traces of the Digital Age. *Voprosy ehkspertnoi praktiki = Issues of Expert Practice*, 2019, no. 51, pp. 423–426. (In Russian). EDN: IFBYGN.

11. Brian J. Network File System Forensic Analysis. Addison-Wesley Professional, 2005. 600 p.

12. Easttom C. Digital Forensics, Investigation and Response. Jones, Bartlett Learning, 2021. 403 p.

13. Nelson B., Steuart C., Phillips A. Guide to Computer Forensics and Investigations. Course Technology, 2018. 688 p.

14. Ham J., Davidoff S. Network Forensics: Tracking Hackers through Cyberspace. Pearson Education, 2012. 576 p.

15. Godwin J., Anzaldua R., Volonino L. Computer Forensics: Principles and Practices. Prentice Hall PTR, 2006. 552 p.

16. Bolvachev M.A. *Use of Social Media in the Investigation of Extremist Crimes. Cand. Diss*. Kaliningrad, 2022. 206 p.

17. Kolycheva A.N., Vasyukov V.F.; Volevodz A.G. (ed.). *Investigation of Crimes with the Use of Computer Information from the Internet.* Moscow, Prospekt Publ., 2022. 200 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Давыдов Владимир Олегович — профессор кафедры правосудия и правоохранительной деятельности Тульского государственного университета, почетный сотрудник МВД России, лауреат премии МВД России в области науки, доктор юридических наук, доцент, г. Тула, Российская Федерация; e-mail: VladDv71@yandex.ru.

INFORMATION ABOUT THE AUTHOR

Davydov, Vladimir O. — Professor, Department of Justice and Law Enforcement Activities, Tula State University, Honorary Member of the Russian Ministry of Internal Affairs, Recipient of the Russian Ministry of Internal Affair's Award for Research, Doctor of Law, Ass. Professor, Tula, the Russian Federation; e-mail: VladDv71@yandex.ru.

ДЛЯ ЦИТИРОВАНИЯ

Давыдов В.О. Цифровое пространство как место совершения преступлений экстремистской направленности / В.О. Давыдов. — DOI 10.17150/2500-4255.2024.18(1).89-95. — EDN ZCLJNS // Всероссийский криминологический журнал. — 2024. — Т. 18, № 1. — С. 89–95.

FOR CITATION

Davydov V.O. Digital Space as a Scene of Extremist Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 1, pp. 89–95. (In Russian). EDN: ZCLJNS. DOI: 10.17150/2500-4255.2024.18(1).89-95.