DOI: 10.17803/1729-5920.2024.214.9.072-083

А. Б. Смушкин
Саратовская государственная юридическая академия
г. Саратов, Российская Федерация

К вопросу о криминалистическом значении отдельных видов компьютерных сетей

Резюме. Констатируя большой криминалистический потенциал компьютерных сетей, автор делит их на шесть типов (по функционалу и уровню обслуживания): нательная (BAN), персональная (PAN), локальная (LAN), кампусная (CAN), городская (MAN) и глобальная сети (WAN). Представляется, что сети уровня BAN и PAN можно условно объединить в единую группу — личные сети (некоторые ее устройства могут входить как в одну, так и в другую сеть или быть элементами обеих одновременно). Сети LAN и CAN логично аккумулировать в группу коллективных сетей, а сети мегаполиса (MAN) и глобальные (WAN) — в группу мультипользовательских сетей. Автор акцентирует внимание на коллективных и мультипользовательских сетях. При этом указывается на необходимость выделения также национального уровня компьютерных сетей. Рассматриваются криминалистически значимые основы функционирования данных сетей. Определяются специфика работы и основные задачи следователя при исследовании сетей различного уровня. Констатируется, что релевантная информация может быть извлечена из сетей практически любого типа. Знание типа, иерархии и уровня охвата сети будет способствовать оптимизации расследования за счет повышения оперативности установления провайдера, администратора и получения от него информации о пользователе сети. По результатам исследования специфики сетей предлагаются общие рекомендации по работе с любым типом сети.

Ключевые слова: криминалистическое исследование сетей; нательная сеть (BAN); персональная сеть (PAN); локальная сеть (LAN); кампусная сеть (CAN); городская сеть (MAN); глобальная сеть (WAN); Интернет; Clearnet; глубокий интернет; криминалистическое исследование Даркнета; установление IP-адреса пользователя; осмотр сетевых ресурсов; дорожка электронно-цифровых следов

Для цитирования: Смушкин А. Б. К вопросу о криминалистическом значении отдельных видов компьютерных сетей. *Lex russica.* 2024. Т. 77. № 9. С. 72–83. DOI: 10.17803/1729-5920.2024.214.9.072-083

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312 (https://rscf.ru/project/24-28-00312/).

Forensic Significance of Certain Types of Computer Networks

Aleksandr B. Smushkin
Saratov State Law Academy
Saratov, Russian Federation

Abstract. Stating the great forensic potential of computer networks, the author differentiates computer networks into 6 types (in terms of functionality and level of service): personal (BAN), personal (PAN), local (LAN), campus (CAN), urban (MAN) and global networks (WAN). It seems that the BAN and PAN level networks can be conditionally combined into a single group — personal networks (some of its devices can be part of both one and the other network or be elements of both at the same time). It is logical to accumulate LAN and CAN networks into a group — collective networks, and megapolis (MAN) and global (WAN) networks into a group — multiuser networks. In the paper, the author focuses on collective and multiuser networks. At the same time, it is also indicated that there is a need to allocate a national level of computer networks. The author examines the criminalistically significant fundamentals of the functioning of the networks under consideration. The paper

determines the specifics of the work and the main tasks of the researcher in the study of networks of various levels. It is stated that relevant information can be extracted from almost any type of network. Awareness of the type, hierarchy and level of network coverage will help optimize the investigation by increasing the speed of identifying the provider, the administrator and obtaining information about the network user from him. Based on the results of the study of network specifics, general recommendations for working with any type of network are offered.

Keywords: forensic investigation of networks; body network (BAN); personal network (PAN); local area network (LAN); campus network (CAN); urban network (MAN); and global network (WAN); Internet; Clearnet; Deep Internet; Forensic investigation of the Darknet; IP address establishment user; inspection of network resources, a track of electronic and digital traces

Cite as: Smushkin AB. Forensic Significance of Certain Types of Computer Networks. *Lex russica*. 2024;77(9):72-83. (In Russ.). DOI: 10.17803/1729-5920.2024.214.9.072-083

Acknowledgments. The research was carried out with the grant of the Russian Science Foundation No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

Введение

Компьютерные сети во многом являются одним из элементов, сокращающих расстояния и укрепляющих связи в социуме. Каждый пользователь и каждое устройство в течение дня подключается к нескольким сетям — домашней, общественной в транспорте или по пути на работу, локальной сети на работе, глобальной (Интернету) и т.д. Криминалистический потенциал компьютерных сетей очень велик. Вопросы их исследования неоднократно попадали в фокус изучения ученых-криминалистов. Так, выделение глобальной сети «Интернет» и локальных сетей как элементов киберпространства отметил еще в 2001 г. в своей диссертации В. А. Мещеряков[1]. При этом самые последние его работы опираются уже на более подробную дифференциацию сетей. Как отмечает В. А. Мещеряков, «объединение отдельных компьютеров в сложные системы и связывание их друг с другом благодаря применению сетевых технологий позволяет получить очень важные с точки зрения практического применения технические свойства этих систем и приводит к почти фантастическим с точки зрения классической криминалистики проявлениям следовой картины»[2].

В. Б. Вехов, предлагая новую отрасль криминалистической техники «криминалистическое компьютероведение», называл также ее подотрасль «криминалистическое исследование компьютерных устройств, их систем и сетей»[3].

Е. Р. Россинская, разработав частную теорию «информационно-компьютерного обеспечения криминалистической деятельности», «криминалистическое исследование компьютерных средств и систем» рассматривает как учение, входящее в новую частную теорию[4].

В своих прежних работах мы также подчеркивали необходимость выделения частной теории «исследования и использования компьютерных сетей (сетевой криминалистики)» как элемента теории «электронной цифровой криминалистики»[5].

---

1 *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. С. 108–110.

2 *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. С. 23.

3 *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. … д-ра юрид. наук. Волгоград, 2008. С. 19.

4 Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков ; под ред. Е. Р. Россинской. М. : Проспект, 2022. С. 58–73.

5 *Смушкин А. Б.* Концептуальные основы частной теории электронной цифровой криминалистики (частной теории собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств) : монография / под общ. ред. В. Б. Вехова. М. : Русайнс, 2022. С. 86.

Основная часть

Классифицировать компьютерные сети можно по различным основаниям.

О. С. Кучин делит сети по географическим критериям на следующие виды:

1) локальные — охватывают территорию одного помещения или здания либо одной соты — зоны действия одной базовой радиостанции;

2) местные — действуют в одном населенном пункте (поселении, районе, городе), в том числе в зоне обслуживания узла сети местной связи — на территории, в пределах которой пользовательское (оконечное) оборудование соединяется или может быть соединено абонентскими линиями со средствами связи одного и того же узла сети местной связи;

3) территориальные — функционируют на уровне субъекта Российской Федерации (республики, края, области), в том числе в зоне обслуживания сети местной связи оператора связи — совокупности зон обслуживания всех узлов сети местной связи одного и того же оператора связи;

4) региональные (территориально распределенные) — охватывают географические территории всех субъектов Российской Федерации, входящих в один федеральный округ, или одну зону действия оператора междугородной связи;

5) национальные — действуют в географических границах отдельно взятого государства или всех зон обслуживания национальных операторов связи;

6) глобальные — охватывают географические границы двух и более государств или зону действия международного оператора связи. В качестве примеров можно привести глобальную компьютерную сеть общего пользования «Интернет», глобальную навигационную спутниковую систему (ГЛОНАСС) и т.д.[6]

П. С. Пастухов по принадлежности и функциональному назначению называет локальные, корпоративные, ведомственные компьютерные сети; глобальную компьютерную сеть «Интернет»[7].

Впрочем, кроме территориального охвата и принадлежности, подобные классификации не выделяют существенных эмерджентных черт каждого вида сетей.

Оптимальным представляется деление сетей по уровню обслуживания на следующие виды:

BAN (Body area network) — нательная сеть, образуемая устройствами, вживленными (установленными) в тело человека или расположенными непосредственно на нем;

PAN (Personal area network) — персональная сеть, образуемая прямым соединением небольшого количества (не более восьми) устройств с помощью беспроводной или проводной коммутации;

LAN (Local area network) — локальная сеть, образуемая через сетевой концентратор или аналогичные устройства компьютерами или иными электронными устройствами, расположенными, как правило, в одном или соседних помещениях; коммутация осуществляется преимущественно проводным способом;

CAN (Campus area network) — кампусная сеть, образуемая несколькими локальными сетями в пределах компактно расположенных строений (студгородок, кампус);

MAN (Megapolis area network) — мегаполисная сеть как объединение локальных и кампусных сетей, а также сеть одного провайдера в пределах поселения или нескольких компактно расположенных поселений;

WAN (Wide area network) — глобальная сеть, допускающая подключение любых сетей и электронных устройств. В настоящее время основная глобальная сеть — это сеть «Интернет».

Некоторые уровни сетей имеют настолько близкий, смежный, взаимопроникающий характер, что их можно рассматривать в рамках единых укрупненных групп. Нам представляется, что сети уровня BAN и PAN можно условно объединить в единую группу — личные сети (некоторые ее устройства могут входить как в одну, так и в другую сеть или быть элементами обеих одновременно). Сети LAN и CAN логично аккумулировать в группу коллективных сетей, а сети мегаполиса (MAN) и глобальные (WAN) — в группу мультипользовательских сетей. С учетом того, что наибольший объем криминали-

[6] Электронные носители информации в криминалистике : монография / под ред. д-ра юрид. наук О. С. Кучина. М. : Юрлитинформ, 2017. С. 167.

[7] *Пастухов П. С.* Криминалистическое исследование электронных носителей информации как новая отрасль технико-криминалистической деятельности // Пермский юридический альманах. 2021. № 4. С. 629.

стически значимой информации, имеющей прямое доказательственное значение, может храниться в последних двух группах, а также того, что нами уже подготовлена статья, посвященная рассмотрению первой группы, в данной публикации мы обратимся к коллективной и мультипользовательской группам.

По типу организации компьютерные сети делятся на централизованные (работающие по принципу «клиент — сервер»), децентрализованные (все узлы которых равнозначны), гибридные (где имеются некоторые узлы, аккумулирующие информацию об адресах других узлов, получив которую пользователи могут перекачивать информацию по прямому соединению).

Релевантная информация может быть извлечена из сетей практически любого типа. Знание типа, иерархии и уровня охвата сети будет способствовать оптимизации расследования за счет повышения оперативности установления провайдера, администратора и получения от него информации о пользователе сети.

Итак, локальная сеть как носитель криминалистически значимой информации может быть интересна следствию с точки зрения как ее иерархии, так и содержащейся в ней информации.

Проводные локальные сети построены в основном по стандартам технологии Ethernet. Беспроводные используют Wi-Fi.

Классическая локальная сеть использует концентратор (хаб), коммутируемая построена на коммутаторах (свитчах). Топология может быть последовательной, общей шиной, звездой и т.д.

Подвидом локальной сети является сеть NAN (Near me area network) — сеть ближнего радиуса действия — логическая беспроводная сеть связи, образованная устройствами, которые могут использовать разные сетевые подключения. Сети NAN делятся на закрытые и глобальные. Закрытые формируются между устройствами, не использующими GPS-системы и обслуживаемые одним оператором. Глобальные используют GPS и подключение к Интернету.

Наиболее ярко специфику локальной сети в плане ее криминалистической емкости отметил В. А. Мещеряков: «Существенными криминалистическими особенностями локальных компьютерных сетей, существенно влияющих на механизм следообразования в них, является распределение данных, ресурсов и программ»[8]. Локальная сеть дает возможность с любого компьютера сети использовать ресурсы входящего в нее более мощного компьютера (используя свой компьютер практически как только терминал для ввода информации и монитор для вывода, знакомиться с информацией, размещенной на ином компьютере, запускать программы с другого устройства, пользоваться периферийными устройствами (распечатывать или сканировать документы) с любого из включенных в сеть компьютеров).

Следователь должен установить сервер / рабочую станцию локальной сети и локализацию разводки коммутационных линий. При этом необходимо принимать во внимание возможность существования, кроме отдельной серверной комнаты, еще небольших серверных локальных узлов.

При исследовании локальной сети определяются:

— скорость передачи информации в ней (по скорости локальные сети Ethernet могут быть разделены на: Ethernet — 10 Мб/с; Fast Ethernet — 100 Мб/с; Gigabit Ethernet — 1 Гб/с; 10G Ethernet — 10 Гб/с; 40-гигабитный и 100-гигабитный Ethernet с одноименным наименованием);

— IP-адреса подключенных к ней устройств. Они могут быть установлены как с помощью командной строки компьютера, так и через сторонние программные предложения, анализирующие сетевой трафик, например Wireless Network Watcher. Кроме того, соответствующая информация может быть изучена и через административную запись маршрутизаторов (данные для входа в которую могут быть расположены на дне или тыльной стороне маршрутизатора). Некоторые антивирусные комплексы сейчас могут показывать устройства, подключенные к локальной сети, и их состояние (активность) (например, некоторые приложения семейства Kaspersky);

— информация, хранящаяся в памяти каждого элемента локальной сети;

— сетевой трафик.

Следователю и специалисту необходимо обнаружить все устройства, подключенные к локальной сети, и исследовать их на предмет криминалистически релевантной информации.

[8] *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике : монография. С. 24.

При этом в случае проводной локальной сети данная задача не вызовет больших сложностей; при выявлении же беспроводной сети WLAN в задачу следствия входит сначала определение количества и типа устройств, подключенных к данной сети, и лишь потом поиск в окружающих помещениях устройств соответствующего типа с выявленным MAC-адресом. Конечно, доступ к иному устройству можно получить и с другого компьютера локальной сети, но это не означает открытость всей информации, всех директорий, а также съемных носителей информации, еще не распознанных или неправильно распознанных системой. Следует согласиться с Е. Р. Россинской, что «элементы локальной сети и целые ее сегменты могут быть разнесены не только по разным помещениям в здании, но и по различным географическим регионам, если для построения сети используется технология VPN (от англ. Virtual Privat Network — виртуальная частная сеть)»[9].

Необходимо определить, имеет ли место изолированная локальная сеть или какое-либо из устройств имеет выход в сеть более высокого уровня. При наличии изолированной сети, когда все ее устройства выявлены и находятся под контролем следователя, можно не производить отключение компьютерных устройств (поскольку нет опасности внешнего воздействия — модификации или уничтожения информации).

В протоколе осмотра подлежат обязательному отражению характер соединения сети, присутствие нештатных устройств. Целесообразно также составить схему подключения и расположения устройств.

Кампусная сеть может быть нескольких категорий:

1) CAN на основе Ethernet;

2) беспроводная CAN на основе технологии Wi-Fi;

3) управляемая CAN (предназначена для обеспечения повышенной безопасности сети и включает брандмауэры, системы обнаружения вторжений и виртуальные частные сети (VPN));

4) CAN с резервными линиями связи для гарантированного обеспечения бесперебойного соединения;

5) CAN с кластеризацией серверов (предполагающая объединение нескольких серверов для работы как единой системы).

Исследование кампусной сети имеет характерные черты, в принципе, сходные с исследованием локальной сети — только с учетом масштабирования на более крупную сеть. Следует отметить, что оперативность действий следователя и специалиста по установлению подключенных локальных сетей и изолированных устройств при выявлении кампусной сети имеет повышенное значение, поскольку большое количество подключенных устройств может осложнить установление их местонахождения и контроля над ними. При этом под угрозу ставится возможность использования фактора внезапности. Представляется необходимым для нивелирования проблемы большого количества устройств, включенных в сеть, расширение круга участников следственной группы и привлечение прежде всего дополнительных специалистов. Сети кампусов — это всегда сети с централизованным управлением, и, соответственно, в задачу следствия также должно входить выявление и блокирование компьютера администратора такой сети.

Зная иерархию локальной или кампусной сети, следователь может получить доступ к интересующему его терминалу и расположенной на нем информации с любого иного устройства и применить полученные данные с максимальным использованием фактора внезапности.

Городская сеть MAN (или сеть мегаполиса) чаще всего имеет выход в глобальную сеть и редко существует самостоятельно и изолированно. Наиболее ярким примером городской сети являются кабельные сети телевещания или опорные сети провайдера. К новейшим направлениям использования городской сети можно отнести «умный» транспорт, «умное» коммунальное хозяйство и иные элементы «умного» города.

Такая сеть в диаметре может составлять от 5 до 100 км. Исследование городской сети по сравнению с рассмотренными выше коллективными сетями отличается не просто масштабированием данной сети и увеличенной территориальной разнесенностью, но и возможностью объединения в ней коллективных

[9] *Россинская Е. Р.* Особенности тактики и технологии осмотра места происшествия при расследовании компьютерных преступлений // Уголовная политика на современном этапе : материалы Международной научно-практической конференции, проходившей в рамках II Байкальского юридического форума, Иркутск, 23–25 сентября 2021 г. Иркутск : Байкальский государственный университет, 2021. С. 181–188.

сетей, бóльшим количеством участников сети и, как следствие, осложнением поиска конкретного фигуранта. Однако при этом городская сеть расположена в пределах одного поселения, что дает возможность более оперативного реагирования, централизованного управления силами и средствами, задействованными для выявления и задержания злоумышленников. А единый провайдер (в отличие от глобальной сети) способствует оптимизации установления IP-адреса пользователя (что облегчит установление его местонахождения), а также персональных данных пользователей сети, зарегистрированных у провайдера.

Представляется необходимым также выделять национальный уровень сети, промежуточный между городской и глобальной сетями, например «Рунет», французскую Minitel. Практически все национальные сети вошли в качестве составных частей в Интернет, а не остались самостоятельными, имея только шлюзы в «большой» Интернет. Однако инфраструктура соответствующих сетей сохранилась, что дает возможность ее эксплуатации при «отрезании» страны от глобальной сети. При этом криминалистически значимыми факторами таких сетей будут: повышение контроля над содержащейся в них информацией (размещение серверов на территории страны), что устраняет фактор неоперативной работы по запросам или вообще игнорирования запросов в недружественных странах, а также фактор стран, с которыми не заключены соответствующие договоры о правовой помощи; возможность привлечения к ответственности владельцев ресурсов, поскольку они находятся чаще всего на территории страны, являются ее гражданами; возможность отслеживания и соответствующей маркировки информации вне сети; облегчение борьбы с фейковой информацией; возможность повышенного контроля социальных сетей, маркетплейсов путем установления повышенной ответственности владельцев и администраторов подобных ресурсов.

Глобальная сеть обеспечивает взаимодействие неограниченного числа пользователей. Основным примером является глобальная сеть «Интернет». Криминалистическое исследование данной сети связано с изучением размещенной в ней информации, установлением пользователя и его местонахождения.

С точки зрения открытости информации глобальная сеть «Интернет» делится на три слоя. Первый слой — «открытый Интернет» (Clearnet) — с проиндексированными источниками, доступ к которым осуществляется с помощью обычных браузеров. Однако, по статистике, на данном слое Интернета размещено всего лишь около 3 % информации.

Второй слой — «глубокий Интернет» (Deepnet или Deep web) — совокупность баз и локальных сетей, не индексируемых поисковыми системами, фактически существующих параллельно Clearnet. В этом слое Интернета находится около 90 % всего ценного научно-технического, технологического, финансово-экономического и государственного открытого контента. Объемы этого слоя Интернета постоянно растут[10].

Третий слой — «темный Интернет» (Darknet) — совокупность ресурсов, доступ к которым осуществляется с повышенной анонимизацией, обеспечиваемой с помощью специальных программных комплексов. Здесь содержится лишь 0,1–1 % информации всего Интернета[11].

Относительно Clearnet И. Н. Воробец вполне обоснованно отмечает, что «характерной особенностью, имеющей определяющее значение для возможности контроля движения информации в сети, является то, что система адресации в сети «Интернет», описываемая IP-протоколом, построена на основе присвоения каждому компьютеру, подключенному к Сети, уникального идентификационного номера (IP-адреса). IP-адрес — это набор из четырех десятичных чисел, отделенных точками (например, 192.168.100.47). Для удобства работы числовые адреса заменяются символьными с использованием доменной системы преобразования имен. Система доменов позволяет преобразовывать символьные имена в IP-адреса и обратно определять имя домена по числовому адресу. IP-адреса могут быть статистическими и динамическими. Размещение в Сети информации, доступ к ней, а также внутрисетевой обмен информацией осуществляется при участии спе-

[10] *Ларина Е. С.*, *Овчинский В. С.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Кн. мир, 2014. С. 5–6.

[11] *Узденов Р. М.* Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 651.

циализированных организаций — поставщиков услуг (провайдеров)»[12].

Следует учитывать, что IP-адрес может иметь как статический, так и динамический характер. При этом С. И. Кувычков указывает: «Так как чаще всего динамический IP-адрес компьютеру, подключаемому к сети, назначается провайдером автоматически, то при разнице во времени, зависящей от временны́х поясов, под данным IP-адресом с интервалом даже в один час могли работать разные пользователи. Судебной практике известны случаи, когда правоохранительные органы, не учитывая указанный момент, изымали компьютерную технику и пытались обвинить людей, не причастных к совершению преступления»[13]. Проверка провайдера, обслуживающего указанные адреса, а также географического нахождения устройства может быть осуществлена и с помощью сетевых ресурсов, таких как, например, WHOIS, RIPE. Однако данные названных сайтов могут иметь лишь ориентирующее, а не доказательственное значение. Существует множество способов сокрытия реального IP-адреса. Чаще всего, конечно, встречается использование VPN-серверов и прокси-серверов. В случае использования прокси-сервера существуют рекомендации по установлению реального IP-адреса:

— принуждение злоумышленника выполнить активный сценарий JavaScript или VBScript, ActiveX, plug-ins для программ-браузеров, программу Java на открываемом сайте, которые могут передавать реальный IP-адрес злоумышленника напрямую, минуя прокси-сервер;

— получение журналов в виде лог-файлов с прокси-сервера путем официальных запросов или с помощью методов интернет-разведки[14].

Применение VPN-серверов осложняет установление реального IP. Ведь сам принцип применения виртуальных частных сетей связан с тем, что шифрованный запрос пользователя провайдер направляет для подключения к виртуальной сети, после чего последующие запросы проходят через эту сеть и от ее имени. Следовательно, следы пользователя уходят из поля зрения провайдера.

Глубокий Интернет в большинстве случаев использует принцип централизованной сети (клиент-серверную организацию). Однако корпоративные файлообменные сети могут иметь и децентрализованный характер.

Даркнет в большей мере использует принцип распределенной информации децентрализованной сети.

В. Б. Вехов выделяет следующие технологии, используемые в Даркнете:

1) специальные поисковые системы (интернет-браузеры);

2) технологии, предназначенные для обмена информацией между пользователями (это так называемые файлообменники и мессенджеры);

3) анонимайзеры;

4) операционные системы специального назначения[15].

При применении TOR используются многослойное шифрование и многоступенчатая передача данных. Как указывают Ю. А. Бондаренко и Г. М. Кизилов, «маршрутизатор в начале передачи информации выбирает случайное число промежуточных маршрутизаторов и генерирует CREATE-сообщения, шифруя их симметричным ключом и указывая для каждого маршрутизатора, какой маршрутизатор будет следующим на пути»[16].

---

[12] *Воробец И. Н.* Глобальная сеть Интернет как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России : доклады междунар. науч.-практ. конференции / под ред. А. М. Кустова, Т. Ю. Прокофьевой. М. : Мэйлер, 2012. С. 71.

[13] *Кувычков С. И.* К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 77.

[14] *Лабутин Н. Г.* Некоторые способы поиска и определения местонахождения злоумышленников в сети Интернет // Математические методы и информационно-технические средства : сборник материалов XI Всероссийской научно-практической конференции. Краснодар, 2014. С. 164–168.

[15] Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024. С. 266–271.

[16] *Бондаренко Ю. А.*, *Кизилов Г. М.* Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. 2019. № 5. С. 99.

Криминалистическому исследованию Даркнета на настоящий момент посвящено не слишком много источников. Так, Российский индекс научного цитирования при поиске информации по подобному запросу выдает не более 20 источников криминалистического характера. Между тем представляется насущно необходимой разработка указанного вопроса, поскольку многие преступления в наше время осуществляются в дистанционном режиме с использованием «темного Интернета», а его повышенная анонимность приводит к неустановлению участников преступления и оставлению преступления нераскрытым.

Среди общих рекомендаций по осмотру сетевых информационных ресурсов можно выделить следующие:

— обязательное привлечение специалиста, поскольку именно он может определить состав локальной или кампусной сети, количество подключенных устройств и многие другие факторы, особенности работы с городской или глобальной сетью;

— скорейшее установление IP-адресов интересующих следствие пользователей. При этом необходимо принимать во внимание существование не только статических, но и динамических (периодически меняющихся при новом подключении) IP-адресов устройств;

— обязательную подготовку электронных носителей с большой емкостью памяти для возможного копирования криминалистически релевантной информации (поскольку даже уже не максимальные, а средние показатели объемов памяти частных электронных устройств сейчас достигают 128–256 Гб для смартфонов, 10–20 Тб для стационарных компьютеров и 1–2 Тб для ноутбуков). При этом использование RAID-массивов еще больше увеличивает емкость памяти соответствующего устройства;

— использование только сертифицированного и принятого на вооружение программно-аппаратного обеспечения, исследующего компьютерную информацию, например программного комплекса «Мобильный криминалист»;

— обязательное наличие в материально-техническом оснащении следственной группы соответствующих «мешков Фарадея» или «клеток Фарадея» для переноса электронных носителей информации с полным блокированием внешнего магнитного, радиоволнового и иного воздействия;

— обязательное исследование сетевых журналов и лог-файлов.

С учетом изложенного можно положительно оценить предложения авторов по разработке и внедрению новых видов следственного осмотра, связанных с осмотром сетевых информационных ресурсов[17]. Свои предложения по данному вопросу мы уже высказывали неоднократно в прежних публикациях[18].

Фактически дорожки электронных цифровых следов при исследовании любых из рассматриваемых видов сетей будут достаточно сходными. В. Б. Вехов отмечает возможность выявления следующих записей, связанных с использованием сетевых подключений, в элементах отдельного компьютерного устройства: записей в файловой системе (реестре операционной системы и др.) компьютера преступника, свидетельствующих о подключении и использовании модема, либо записей, содержащихся в модуле идентификации абонента и аппарата связи в компьютерной сети оператора; записей в памяти компьютера или аппарата связи преступника; записей в памяти коммутационного компьютерного устройства контроля, авторизации и аутентификации абонентов в сети оператора(-ов) связи; записей в автоматической системе учета данных для начисления платы за оказанные услуги связи; записей, автомати-

[17] См.: *Першин А. Н.* Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. 2020. № 1. С. 13–16 ; *Сысенко А. Р.*, *Герасименко Н. И.* Особенности осмотра информации, хранящейся на ресурсах сети Интернет // Закон и право. 2022. № 7. С. 214–217 ; *Иванов А. Н.* Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. Новая серия. Серия «Экономика. Управление. Право». 2009. Т. 9. № 2. С. 74–77 ; Высокотехнологичный уголовный процесс : монография / под ред. д-ра юрид. наук С. В. Зуева, д-ра юрид. наук Л. Н. Масленниковой. М. : Юрлитинформ, 2023. С. 69.

[18] См.: *Смушкин А. Б.* Современное состояние «электронных» следственных действий в России // Вызовы информационного общества: тенденции развития правового регулирования цифровых трансформаций : монография по материалам 4.0 Международной научно-практической конференции (г. Саратов, 24–25 мая 2023 г.) / под ред. Н. Н. Ковалевой. Саратов : Изд-во Сарат. гос. юрид. акад., 2023. С. 216–225 ; *Он же.* Концепция дистанционной криминалистики. М. : Юрлитинформ, 2024 ; *Он же.* Концеп-

чески регистрируемых в журнале событий компьютерной сети, который находится на сервере оператора связи в ве́дении администратора сети; записей, автоматически образующихся в памяти транзитных технологических устройств различных операторов при сопряжении с их сетями передачи данных по протоколу IP; записей в памяти серверов (FTP, SMTP, POP3 и др.) оператора связи, обслуживающего абонентский терминал потерпевшего, о входящих на него вызовах, соединениях и передачах компьютерной информации (электронных сообщений, электронных почтовых отправлений и др.), а также дистанционном управлении его информационными ресурсами; записей в файловой системе (реестре операционной системы и др.) компьютера потерпевшего о параметрах изменения подключения модема, настроек браузера, а также о нарушении режима работы или дезактивации средств защиты портов и компьютерной информации; записей в памяти компьютера или аппарата связи потерпевшего, содержащих сведения о полученной компьютерной информации, вредоносных программах, несанкционированном изменении системного и прикладного программного обеспечения, а также компьютерной информации потерпевшего либо сбоях в работе ЭВМ, его программного обеспечения и периферийного оборудования[19].

Конечно, научно-технический прогресс не стоит на месте, и отдельные элементы сетей сейчас изменились (так, практически не используются модемы), но сам принцип изучения дорожки электронных следов в сети остается актуальным и по сей день.

Следует также согласиться с Е. Р. Россинской по вопросу о возможности применения в ходе такого изучения субъективного метода осмотра, выражающегося в данном случае в движении по цифровым следам, оставленным в сети, начиная от скомпрометированной станции, далее по цепочке других компьютеров и серверов до устройства, с которого началось проникновение[20].

Заключение

Резюмируя изложенное, можно отметить, что знание следователем специфики осматриваемой сети будет способствовать минимизации риска ошибок, связанных с тратами времени на «пустое» устройство и, соответственно, с потерей фактора внезапности в отношении владельцев иных устройств, включенных в данную сеть. Конечно, в глобальных сетях подобный риск снижается, однако имеют место другие риски: так, А. К. Жарова отмечает, что «разработаны программные технологии, которые позволяют менять IP-адрес, например, возможно создавать динамические, или “невидимые”, или нераспознаваемые IP-адреса»[21].

СПИСОК ЛИТЕРАТУРЫ

Бондаренко Ю. А., *Кизилов Г. М.* Проблемы выявления и использования следов преступлений, оставляемых в сети Darknet // Гуманитарные, социально-экономические и общественные науки. 2019. № 5. С. 97–101.

Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. … д-ра юрид. наук. Волгоград, 2008. 45 с.

Воробец И. Н. Глобальная сеть Интернет как пространство для совершения преступлений // Экономические, правовые и прикладные аспекты преодоления кризиса в европейских странах и России : доклады междунар. науч.-практ. конференции / под ред. А. М. Кустова, Т. Ю. Прокофьевой. М. : Мэйлер, 2012. С. 68–73.

Высокотехнологичный уголовный процесс : монография / под ред. д-ра юрид. наук С. В. Зуева, д-ра юрид. наук Л. Н. Масленниковой. М. : Юрлитинформ, 2023. 216 с.

ция «электронных» следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. № 3 (19). С. 165–173.

[19] *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. … д-ра юрид. наук. Волгоград, 2008. С. 34.

[20] Теория информационно-компьютерного обеспечения криминалистической деятельности. С. 95.

[21] *Жарова А. К.* О соотношении персональных данных с IP-адресом. Российский и зарубежный опыт // Вестник УрФО. Безопасность в информационной сфере. 2016. № 1. С. 61–67.

Жарова А. К. О соотношении персональных данных с IP-адресом. Российский и зарубежный опыт // Вестник УрФО. Безопасность в информационной сфере. 2016. № 1. С. 61–67.

Иванов А. Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. Новая серия. Серия «Экономика. Управление. Право». 2009. Т. 9. № 2. С. 74–77.

Кувычков С. И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 76–81.

Лабутин Н. Г. Некоторые способы поиска и определения местонахождения злоумышленников в сети Интернет // Математические методы и информационно-технические средства : сборник материалов XI Всероссийской научно-практической конференции. Краснодар, 2014. С. 164–168.

Ларина Е. С., *Овчинский В. С.* Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Кн. мир, 2014. 380 с.

Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.

Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. 176 с.

Пастухов П. С. Криминалистическое исследование электронных носителей информации как новая отрасль технико-криминалистической деятельности // Пермский юридический альманах. 2021. № 4. С. 622–639.

Першин А. Н. Осмотр сетевых информационных ресурсов — новый вид следственного действия? // Российский следователь. 2020. № 1. С. 13–16.

Россинская Е. Р. Особенности тактики и технологии осмотра места происшествия при расследовании компьютерных преступлений // Уголовная политика на современном этапе : материалы Международной научно-практической конференции, проходившей в рамках II Байкальского юридического форума, Иркутск, 23–25 сентября 2021 г. Иркутск : Байкальский государственный университет, 2021. С. 181–188.

Смушкин А. Б. Концепция «электронных» следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. № 3 (19). С. 165–173.

Смушкин А. Б. Концептуальные основы частной теории электронной цифровой криминалистики (частной теории собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств) : монография / под общ. ред. В. Б. Вехова. М. : Русайнс, 2022. 222 с.

Смушкин А. Б. Концепция дистанционной криминалистики. М. : Юрлитинформ, 2024. 256 с.

Смушкин А. Б. Современное состояние «электронных» следственных действий в России // Вызовы информационного общества: тенденции развития правового регулирования цифровых трансформаций : монография по материалам 4.0 Международной научно-практической конференции (г. Саратов, 24–25 мая 2023 г.) / под ред. Н. Н. Ковалевой. Саратов : Изд-во Сарат. гос. юрид. акад., 2023. 216–225.

Сысенко А. Р., *Герасименко Н. И.* Особенности осмотра информации, хранящейся на ресурсах сети Интернет // Закон и право.2022. № 7. С. 214–217.

Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков ; под ред. Е. Р. Россинской. М. : Проспект, 2022. 256 с.

Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 649–655.

Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024. 491 с.

Электронные носители информации в криминалистике : монография / под ред. д-ра юрид. наук О. С. Кучина. М. : Юрлитинформ, 2017. 300 с.

REFERENCES

Bondarenko YuA, Kizilov GM. Problems of identifying and using traces of crimes left on the Darknet network. *Humanities, Socio-Economic and Social Sciences*. 2019;5:97-101. (In Russ.).

Ivanov AN. Remote computer information research: criminal procedural and criminalistic problems. *Proceedings of the Saratov University. The Economics series. Management. Law*. 2009;9(2):74-77. (In Russ.).

Kuchina OS (ed.). Electronic media in criminalistics. Moscow: Yurlitinform Publ.; 2017. (In Russ.).

Kuvychkov SI. On the issue of the use of electronic information in criminal procedural evidence: theoretical and applied aspect. Legal science and practice: *Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 2015;2(30):76-81. (In Russ.).

Labutin NG. Some ways of searching and locating intruders on the Internet. *Mathematical methods and information technology tools: Collection of proceedings of the 11th All-Russian scientific and practical conference*. Krasnodar; 2014. (In Russ.).

Larina ES. Cyber wars of the 21st century. What Edward Snowden didn't say. Moscow: Knizhnyi mir Publ.; 2014. (In Russ.).

Meshcheryakov VA. Fundamentals of the methodology for investigating crimes in the field of computer information. Dr. Sci. Diss. Voronezh; 2001. (In Russ.).

Meshcheryakov VA. Theoretical foundations of the mechanism of trace formation in digital criminology. Moscow: Prospekt Publ.; 2022. (In Russ.).

Pastukhov PS. Forensic research of electronic media as a new branch of technical and forensic activity. *Perm Legal Almanac*. 2021;4:622-639. (In Russ.).

Pershin AN. Inspection of network information resources — a new type of investigative action? *Russian Investigator*. 2020;1:13-16. (In Russ.).

Rossinskaya ER, Semikalenova AI, Ryadovsky IA, Saakov TA. Rossinskaya ER (ed.). Theory of information and computer support for criminalistic activities. Ministry of Science and Higher Education of the Russian Federation; Kutafin Moscow State Law University (MSAL). Moscow: Prospekt Publ.; 2022. (In Russ.).

Rossinskaya ER. Features of tactics and technology of scene inspection in the investigation of computer crimes. In: Rossinskaya ER. Criminal policy at the present stage: *Proceedings of the International scientific and practical conference held within the framework of the 2nd Baikal Legal Forum*, Irkutsk, September 23–25, 2021. Irkutsk: Baikal State University; 2021. (In Russ.).

Smushkin AB. The concept of «electronic» investigative actions. *Criminalistics: Yesterday, Today, Tomorrow.* 2021;3(19):165-173. (In Russ.).

Smushkin AB. The concept of remote criminology. Moscow: Yurlitinform Publ.; 2024. (In Russ.).

Smushkin AB. The current state of «electronic» investigative actions in Russia/Challenges of the Information Society: trends in the development of legal regulation of digital transformations: Monograph based on Proceedings of 4.0 of the International Scientific and Practical Conference (Saratov, May 24–25, 2023). Kovaleva NN (ed.). Saratov State Law Academy. Saratov: Publishing House of Saratov State Law Academy; 2023. (In Russ.).

Smushkin AB. Vekhov VB (ed.). Conceptual foundations of the private theory of electronic digital forensics (private theory of collecting, researching and using electronic digital information and information technology devices). Moscow: Rusains Publ.; 2022. (In Russ.).

Sysenko AR, Gerasimenko NI. Features of inspection of information stored on Internet resources. *Zakon i pravo.* 2022;7:214-217. (In Russ.).

Uzdenov RM. New frontiers of cybercrime. *All-Russian Journal of Criminology.* 2016;10(4):649-655. (In Russ.).

Vekhov VB [et al.]. Vekhov VB, Zuev SV (eds.). Digital criminalistics: Textbook for universities. 2nd ed. Moscow: Yurait Publishing House; 2024. (In Russ.).

Vekhov VB. Criminalistic doctrine of computer information and means of its processing. Author's Abstract. Dr. Sci. (Law) Diss. Volgograd; 2008. (In Russ.).

Vorobets IN. The global Internet as a space for committing crimes. In: Kustov AM, Prokofieva TY (eds.). *Economic, legal and applied aspects of overcoming the crisis in European countries and Russia: Reports of the International Scientific and Practical Conference*. Moscow: MAILER Publ.; 2012. (In Russ.).

Zharova AK. About the relationship of personal data with an IP address. Russian and foreign experience. *Journal of the Ural Federal District Information Security.* 2016;1:61-67. (In Russ.).

Zueva SV, Maslennikova LN (eds.). High-tech criminal procedure. Moscow: Yurlitinform Publ.; 2023. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Смушкин Александр Борисович, кандидат юридических наук, доцент, доцент кафедры криминалистики Саратовской государственной юридической академии
д. 1, Вольская ул., г. Саратов 410056, Российская Федерация
skif32@yandex.ru

INFORMATION ABOUT THE AUTHOR

Aleksandr B. Smushkin, Cand. Sci. (Law), Associate Professor, Department of Criminology, Saratov State Law Academy, Saratov, Russian Federation
skif32@yandex.ru

Материал поступил в редакцию 24 апреля 2024 г.
Статья получена после рецензирования 29 апреля 2024 г.
Принята к печати15 августа 2024 г.

Received 24.04.2024.
Revised 29.04.2024.
Accepted 15.08.2024.