УДК / UDC 343
DOI: 10.34076/22196838_2025_1_40

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ УРОВНЕЙ BAN И PAN*

Смушкин Александр Борисович
Ведущий специалист проектного офиса научных программ и исследований, доцент кафедры криминалистики Саратовской государственной юридической академии (Саратов), кандидат юридических наук, доцент, ORCID: 0000-0003-1619-8325, e-mail: Skif32@yandex.ru.

Автор констатирует расширение спектра криминалистически значимой информации, которая может быть использована для расследования преступлений и обеспечения кибербезопасности и личной безопасности граждан за счет сетевой информации. При рассмотрении основных монографических исследований, связанных с выделением сетевой криминалистики (криминалистического исследования компьютерных систем и сетей) в качестве самостоятельного раздела, указано, что до последнего времени исследованию подвергались лишь глобальная сеть Интернет и отчасти локальные сети. Между тем выделяется более широкий спектр сетей по функционалу и уровню обслуживания: нательная (BAN), персональная (PAN), локальная (LAN), кампусная (CAN), городская (MAN) и глобальная сети (WAN). Основное внимание уделено двум первым уровням компьютерных сетей, имеющим непосредственную взаимосвязь с конкретным человеком. Утверждается, что релевантная информация может быть извлечена из сетей практически любого типа. Рассмотрены криминалистические аспекты выявления и исследования данных сетей, а также их применения. Анализируется возможность использования этих сетей для несомненной идентификации человека, оценки действий в определенный момент времени и др. Электронная природа обозначенной информации характеризует возможность ее трансформации в электронные доказательства в различных видах судопроизводства.

Ключевые слова: сетевая криминалистика, нательная компьютерная сеть body area network (BAN), персональная компьютерная сеть personal area network (PAN), обнаружение сетей, виртуальные следы, цифровая информация

Для цитирования: Смушкин А. Б. Криминалистические аспекты исследования компьютерных сетей уровней BAN и PAN // Электронное приложение к «Российскому юридическому журналу». 2025. № 1. С. 40–49. DOI: https://doi.org/10.34076/22196838_2025_1_40.

FORENSIC ASPECTS OF THE STUDY OF COMPUTER NETWORKS OF THE BAN AND PAN LEVELS**

Smushkin Alexander
Leading specialist of the project office of scientific programs and research, associate professor, Saratov State Law Academy (Saratov), candidate of legal sciences, ORCID: 0000-0003-1619-8325, e-mail: Skif32@yandex.ru.

During the research, the author states the expansion of the range of criminally significant information that can be used to investigate crimes and ensure cybersecurity and personal safety of citizens through network information. Considering the main monographic studies related to the allocation of network criminology (forensic research of computer systems and networks) as an independent section, it is stated that until recently only the global Internet and partly local networks have been studied. Meanwhile, a wider range of networks stands out in terms of functionality

* Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, URL: https://rscf.ru/project/24-28-00312.

** The research was carried out at the expense of a grant from the Russian Science Foundation № 24-28-00312, URL: https://rscf.ru/project/24-28-00312.

and service level: body (BAN), personal (PAN), local (LAN), campus (CAN), urban (MAN) and global networks (WAN). The main research is devoted to the first two levels of computer networks that have a direct relationship with a specific person. It is stated that relevant information can be extracted from networks of almost any type. The criminalistic aspects of the identification and research of these networks, as well as their application, are considered. The possibility of using these networks for the undoubted identification of a person, assessment of actions at a certain point in time, use as a kind of «Polygraph», etc. is stated. The electronic nature of the information under consideration characterizes the possibility of its transformation into electronic evidence in various types of legal proceedings.

Key words: network forensics, body area network (BAN), personal area network (PAN), network detection, virtual traces, digital information

For citation: Smushkin A. (2025) Forensic aspects of the study of computer networks of the BAN and PAN levels. In *Elektronnoe prilozhenie k «Rossiiskomu yuridicheskomu zhurnalu»*, no. 1, pp. 40–49, DOI: https://doi.org/10.34076/22196838_2025_1_40.

Компьютерные сети окружают нас постоянно. Они могут различаться целевым предназначением, архитектурой и уровнем территориального объединения. 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»[1]. Данное обстоятельство способствует расширению спектра криминалистически значимой информации, которая может быть использована для расследования преступлений и обеспечения кибербезопасности, а также личной безопасности граждан.

Конечно, речь стоит вести об объединении не только компьютеров, но и иных электронных устройств.

Отдельные вопросы криминалистического исследования компьютерных сетей поднимались в науке криминалистике и ранее. Так, предлагая в своей диссертации на соискание ученой степени доктора юридических наук новую частную теорию, «криминалистическое компьютероведение», В. Б. Вехов в качестве одного из составляющих ее учений назвал подотрасль «криминалистическое исследование компьютерных устройств, их систем и сетей»[2]. Е. Р. Россинская предлагает «криминалистическое исследование компьютерных средств и систем» как учение, входящее в новую частную теорию «информационно-компьютерного обеспечения криминалистической деятельности»[3]. Свой вклад в исследование компьютерных сетей внесли и другие ученые. Однако до последнего времени изучались лишь глобальная сеть Интернет и отчасти локальные сети. В настоящее время теоретики и практики в области компьютерной информации не ограничиваются выделением только этих видов сетей.

Для разработок криминалистического плана в области сетевой криминалистики необходимо понимание, что по уровню покрытия компьютерные сети могут быть следующими:

body area network (BAN) – нательная компьютерная сеть. Ее образуют различного рода устройства, вживленные в тело человека или расположенные непосредственно на нем;

personal area network (PAN) – персональная компьютерная сеть: объединение электронных устройств и гаджетов, расположенных в пределах от непосредственно

[1] *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике: моногр. М.: Проспект, 2022. С. 23.

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

[3] Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков; под ред. Е. Р. Россинской; Министерство науки и высшего образования Российской Федерации; Московский гос. юрид. ун-т им. О. Е. Кутафина (МГЮА). М.: Проспект, 2022. С. 58–73.

вплотную к телу человека или в нескольких сантиметрах от тела человека до нескольких метров;

local area network (LAN) – локальная сеть, которую образуют несколько компьютерных устройств, принадлежащих, как правило, одному физическому или юридическому лицу и расположенных в одном или в соседних помещениях;

campus area network (CAN) – кампусная сеть или сеть, объединяющая несколько локальных сетей в пределах относительно небольшой территории;

metropol area network (MAN) – компьютерная сеть, представляющая собой совокупность локальных и кампусных сетей в пределах одного населенного пункта;

wide area network (WAN) – глобальная компьютерная сеть, обладающая возможностями подключения любых компьютерных устройств и любых сетей.

Согласно обозначенной теме исследования наибольший интерес у нас вызвали два первых уровня компьютерных сетей, имеющих непосредственную взаимосвязь с конкретным человеком. Условно данные сети можно назвать термином «личные», сети уровня LAN и CAN – коллективные, а MAN и WAN – сети мультипользователей.

Естественно, из сетей любого уровня может быть извлечена криминалистически релевантная информация. Обнаружение, фиксация и исследование информация сетей body area network и personal area network может осуществляться, как правило, в рамках оперативно-розыскных мероприятий «Снятие информации с технических каналов связи» и «Получение компьютерной информации» или следственного действия «Осмотр места происшествия». Элементы нательной сети body area network могут быть также обнаружены в ходе освидетельствования лица.

Body area network (BAN), или нательная сеть, может быть использована в уголовном судопроизводстве в следующих направлениях.

1. Она может предоставить качественную, четко идентифицирующую человека информацию, «зашитую» в ее устройствах: совокупность идентификационных признаков, образующих идентификационное поле с учетом того, что уже не только в правоохранительной сфере, но и в банковской и некоторых иных коммерческих сферах активно внедряются разработки в области идентификации по цифровым отпечаткам компьютерных устройств[1], позволяющие рассматривать цифровой отпечаток как идентификационную совокупность, характеризующую определенное цифровое устройство с помощью как уникальных параметров, так и не уникальных, но представленных в уникальных сочетаниях. Данные параметры подвергаются хэшированию: преобразуются в строку фиксированной длины, состоящую из цифр и букв, которая может быть сопоставлена для идентификации устройства с другой вычисленной хэш-функцией.

2. Возможно извлечение из нее информации, показывающей повышенную реакцию на какие-либо вопросы или действия следователя. В. А. Мещеряков вообще допускает использование подобной сети в качестве своеобразного постоянно носимого полиграфа[2].

3. Поскольку нательная сеть аккумулирует информацию о показателях организма (давление, сердцебиение, уровень сахара в крови и т. д.), извлеченная из памяти аккумулирующего устройства информация может косвенно указать на повышение физической активности либо стрессовую ситуацию. Данная информация может быть косвенным доказательством волнения, наличия физических нагрузок (бега, борьбы и т. д.), изменения эмоционального состояния, приема пищи, введения лекарственного препарата в интересующее следствие время.

4. Объединение электронных датчиков киберпротезов может даже зафиксировать уровень мышечных усилий, воспроизводимых киберпротезом в конкретное время, что может свидетельствовать о совершении определенных действий. При сопоставлении с механизмом преступления, в котором заподозрено лицо, следствием может быть сделан вывод о факте и объеме физической нагрузки на киберпротез во временной период совершения преступления.

---

[1] Стандарт Банка России СТО БР БФБО-1.7-2023 «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» (принят и введен в действие приказом Банка России от 1 марта 2023 г. № ОД-335 «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023») // Центральный банк Российской Федерации: офиц. сайт. URL: https://cbr.ru/Crosscut/LawActs/File/6177 (дата обращения: 15.07.2024).

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

5. В некоторых случаях вживляемые в тело человека электронные устройства могут содержать в себе датчик геопозиционирования для скорейшего обнаружения в случае приступа, что позволит правоохранительным органам отследить местонахождение или перемещение интересующего их лица в определенный момент или за временной период.

В наиболее общем виде данные сети состоят из сенсорных узлов, сетевых координаторов и исполнительных устройств, связанных между собой радиоинтерфейсом.

Современные нательные сети могут для контроля показателей сопрягаться с внешним устройством. Уже сейчас имеются разработки, аккумулирующие информацию киберпротезов и электростимуляторов на внешние устройства и активизирующие определенный стимулятор или протез, вводящие, например, инсулин больному диабетом, находящемуся в предкоматозном состоянии или в коме и не способному самостоятельно принять меры. В связи с этим насущно важен вопрос возможности перехвата управления указанными устройствами, что уже однажды демонстрировалось, например, в отношении кардиостимуляторов[1]. Разработка действенных мер обеспечения безопасности нательных сетей от несанкционированного проникновения в систему неотъемлемо способствует обеспечению личной безопасности носителей подобной сети. Представляется, что с юридической точки зрения разработка повышенной ответственности за причинение вреда здоровью человека или получение личной информации (например, о болезнях, генетических предрасположенностях и т. д.) путем дополнения соответствующих статей квалифицирующим признаком «с использованием компьютерных устройств» будет фактором общей и частной превенции. В ближайшей перспективе с развитием нанотехнологий сеть BAN можно будет считать одним из основных источников информации о человеке.

Сеть body area network – это технологии, которые могут быть имплантированы в тело человека или размещены непосредственно на нем. Небольшой размер и малая потребляемая мощность предоставляют возможность использовать их в различных целях: от медицинского мониторинга состояния здоровья человека и точечного воздействия (например, введение баклофенака в спинной мозг людей с патологическим напряжением мышц), а также превентивного извещения медиков о критичных изменениях состояния здоровья пациента до анализа показателей эффективности работы организма спортсменов, уровня мобилизации, усталости и иных показателей сотрудников органов безопасности, специальных подразделений, военных, а в ближайшей перспективе прямой беспроводной связи и управления мозгом человека любыми механизмами. Так, китайские ученые[2], а также компания Илона Маска «Neuralink» уже провели эксперименты по вживлению нейрочипов в мозг человека и управлению электронными устройствами[3].

Технологии body area network имеют преимущественно беспроводное соединение. Сеть из миниатюрных сенсорных блоков (BSU) объединена с центральным блоком тела (BCU). Часть из них уже давно разработана и используется (например, кардиостимуляторы), часть только находится в экспериментальной стадии (нейрочипы и т. п.), а часть только просматривается в относительно ближайшей либо отдаленной перспективе (наноботы и пр.).

Типичная BAN сейчас состоит из аппаратов контроля жизненно важных функций, детекторов движения, акселерометров, процессора, приемо-передающего устройства. Эти устройства имеют элементы памяти, информация которых может быть ис-

[1] Взлом с угрозой для жизни // Умная страна. URL: https://umstrana.ru/technology/vzlom-s-ugrozoy-dlya-zhizni/ (дата обращения: 10.04.2024).

[2] Еще 24 октября 2023 г. ученые компании «Neural Electronic Opportunity (NEO)» провели успешный эксперимент по управлению киберпротезом с помощью вживленного нейрочипа. См.: *Bela V.* Chinese brain chip helps paralysed man regain mobility – and it's less invasive than Elon Musk's Neuralink // South China Morning Post. URL: https://www.scmp.com/news/china/science/article/3250476/chinese-brain-chip-helps-paralysed-man-regain-mobility-and-its-less-invasive-elon-musks-neuralink?module=top_story&pgtype=homepage (дата обращения: 10.04.2024).

[3] Илон Макс в интервью компании «Рейтер» официально объявил, что пациент с внедренным в мозг нейрочипом смог управлять компьютерной мышью. См.: Neuralink's first human patient able to control mouse through thinking, Musk says // Reuters. URL: https://www.reuters.com/business/healthcare-pharmaceuticals/neuralinks-first-human-patient-able-control-mouse-through-thinking-musk-says-2024-02-20/ (дата обращения: 10.04.2024).

пользована в целях уголовного судопроизводства (при условии ее грамотного получения в ходе соответствующих следственных действий или ОРМ). Наиболее актуальным представляется учет в тактике производства следственных действий данных обстоятельств, как минимум при выборе привлекаемого специалиста соответствующего профиля. Так, необходимо привлечение не только специалиста технического профиля, но и других: кардиологов, эндокринологов, специалистов по киберпротезированию и т. д.

Связь элементов сети BAN может быть узкополосной (narrowband) NB-PHY; сверхширокополосной (ultra wideband) UWB-PHY; связь по телу человека HBC-PHY. Соответственно, различаться будут как методы выявления людей, оснащенных устройствами BAN, извлечения информации из этой сети в целях судопроизводства, так и защищенность от несанкционированного криминального вмешательства в функционирование устройств сети.

Анализ западных публикаций по проблемам использования сети BAN дает основания к выделению следующих проблемных аспектов:

сложность обеспечения конфиденциальности и безопасности информации;

нерешенные вопросы автоматизации системы валидации датчиков;

отдельные проблемы взаимодействия элементов системы между собой;

сложность обеспечения беспрепятственной передачи данных и подключения к сети Интернет;

недостаточная энергоемкость датчиков;

необходимость не только статического, но и динамического наблюдения за пациентами;

необходимость повышения помехоустойчивости, снижения фрагментированности и нивелирования влияния дефектов в показаниях датчиков на согласованность и качество данных;

перманентное усложнение архитектуры сети body area network, повышающее сложность новых разработок и проектирования;

необходимость снижения влияния иных узлов и датчиков системы на эффективность конкретного датчика;

психологические проблемы неуверенности пациентов и иных пользователей в безопасности при использовании нательных сетей[1].

Отдельным криминалистически значимым направлением можно считать внедрение человеку информационных чипов. Так, в Швеции все более широкое распространение получают чипы, несущие в своей памяти личные документы (ковидный паспорт и т. д.) или банковские чипы, обеспечивающие доступ к счету[2].

Чипы могут быть выполнены из биосовместимого стекла или из силикона. Чипы из биосовместимого стекла в основном используют технологию RFID. Силиконовые чипы могут быть двух типов: RFID или NFC. Первые используются для обеспечения бесключевого доступа к помещению или бесключевого зажигания в автомобиле, вторые – для хранения информации. С криминалистической точки зрения практика показывает, с одной стороны, возможность использования чипов обоих типов для взлома внешнего оборудования, а с другой – возможность атак клонированием на данные чипы для получения доступа к тем или иным объектам. Конечно, стоимость такого клонирования существенно превышает иные варианты взлома и доступа к имуществу частных лиц, однако этот метод вполне может использоваться в целях коммерческого шпионажа. Кроме того, есть программные средства перепрограммирования модулей NFC, например NFC Tools Pro. Таким образом, копирование и вынос секретной информации, компрометация доступа, иные противоправные действия могут быть совершены с использованием этих перепрошитых чипов.

Для расследования преступлений, совершенных с использованием подобных чипов, датчиков, сенсорных устройств системы body area network, представляется ра-

[1] Body area network projects // PhDservices. URL: https://phdservices.org/body-area-network-projects/ (дата обращения: 10.04.2024)

[2] *Басов В.* Хроники чипирования: как люди вживляют в себя микрочипы и можно ли сделать это незаметно // MAXIM. URL: https://www.maximonline.ru/lifestyle/khroniki-chipirovniya-kak-lyudi-vzhivlyayut-v-sebya-mikrochipy-i-mozhno-li-sdelat-eto-nezametno-id521598/ (дата обращения: 10.04.2024); *Grauer Y.* A practical guide to microchip implants // ARSTECHNICA. URL: https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/ (дата обращения: 10.04.2024).

зумным использование рекомендаций цифровой криминалистики по работе с виртуальными следами[1]. Непосредственно в отношении способов криминалистического изучения данных нательных сетей можно отметить следующее.

1. Любые действия носителя нательной сети или в отношении сети, вживленной в носителя либо размещенной на нем, отображаются в виде виртуальных следов в памяти устройств сети.

2. Любая информация, входящая в систему, может быть обнаружена либо на внешнем устройстве управления системой, либо на встроенных чипах.

3. При возникновении интереса следствия к этой информации с помощью специалистов должно быть осуществлено определение наличия вживленных или расположенных на теле человека устройств и чипов системы BAN.

4. При обнаружении сети BAN подключение к соответствующим устройствам и считывание из памяти этих устройств журнала их работы, а также иной интересующей следствие информации и данных, имеющих признаки внешнего вмешательства, производится специалистом с использованием рекомендаций цифровой криминалистики.

5. Обнаруженные элементы нательной сети должны быть описаны с помощью специалиста с точки зрения типа, количества подключенных устройств, иерархии подключения, скорости подключения и т. д. Однако следует учитывать, что датчики не всегда имеют вывод в мобильное приложение, в некоторых случаях их практически невозможно выявить внешними устройствами без полного контакта сканирующего устройства с телом исследуемого лица.

6. Считывание информации осуществляется программно-аппаратными комплексами серии «Мобильный криминалист».

7. Полученная информация может быть обработана алгоритмами, в том числе с использованием методов анализа больших данных и визуализирована в виде графиков, диаграмм, хронологической развертки изменения параметров.

8. Необходимо активизировать разработки в области дистанционного считывания информации в режиме реального времени, что может способствовать использованию нательной сети в качестве несомненного идентификатора человека, а также полиграфа, где под полиграфом подразумевается многопишущее устройство, фиксирующее разнообразные реакции человека на различные внешние раздражители.

Технология сети personal area network (PAN) объединяет домашние личные электронные устройства в количестве не более восьми устройств в единую, централизованную, самоорганизующуюся динамическую сеть, которая характеризуется некоторой аморфностью образования. Как отметил В. А. Мещеряков, «сеть возникает за счет соединения клиентских устройств „на лету“, когда каждый узел пытается передать данные, предназначенные другим узлам». При этом кому именно передать данные в текущий момент, определяется в зависимости от динамически сложившейся связности сети[2].

Сеть personal area network обычно не включает маршрутизатор, следовательно, не имеет выхода в глобальную сеть Интернет. Но одно или несколько устройств этой сети могут входить в сеть более высокого уровня (локальная сеть), которая, соответственно, может иметь выход в сеть Интернет. По используемым технологиям сеть PAN дифференцируется на две основные группы:

---

[1] *Федотов Н. Н.* Форензика – компьютерная криминалистика. М.: Юрид. мир, 2007; *Яковлев А. Н.* Теоретические и методические основы экспертного исследования документов на машинных носителях информации: дис. ... канд. юрид. наук. Саратов, 2000; *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д-ра юрид. наук. Воронеж, 2001; *Агибалов В. Ю.* Виртуальные следы в криминалистике и уголовном процессе: моногр. М.: Юрлитинформ, 2012. 152 с.; *Милашев В. А.* Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: дис. ... канд. юрид. наук. М., 2004; *Мещеряков В. А.* Теоретические основы механизма следообразования в цифровой криминалистике; Теория информационно-компьютерного обеспечения криминалистической деятельности; Цифровые следы преступлений: моногр. М.: Проспект, 2021; *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: моногр. Волгоград: ВА МВД России, 2008; *Смушкин А. Б.* Цифровизация криминалистической деятельности: учеб. пособие / под ред. В. Б. Вехова. М.: КноРус, 2024; *Нестеров А. В.* Виртуальные следы в криминалистике: учеб. М.: КноРус, 2024.

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

беспроводная виртуальная сеть (WPAN): основой использования такой сети являются технологии Bluetooth, инфракрасного соединения, сверхширокополосного соединения, ZigBee и т. д.;

проводная сеть: связь поддерживается с помощью технологии USB или Firewire.

К технологиям personal area network относится соединение, например, мультимедийных устройств (наушников со смартфонами), объединение домашних устройств в единую сеть (умный пылесос, принтер и т. д.), использование объектов категории «Интернет вещей» (IoT), технологии домашнего офиса.

Беспроводная сеть WPAN может иметь различную топологию и быть реализованной по типу звезды, древовидной или ячеистой топологии.

Криминалистическое значение имеет дифференциация данных сетей по скорости стандарта подключения, которая бывает следующей:

высокоскоростная беспроводная сеть HR-VPN: реализует технологию стандарта IEEE-802.15.3 и развивает скорость до 20 Мбит/с;

среднескоростная сеть MR-WPAN: реализует стандарт IEEE 802.15.1 с развитием скорости потока до 1 Мбит/с;

низкоскоростное интернет-соединение LR-VPN: реализуется по технологии IEEE 802.15.4 и развивает скорость не более 25 Кбит/с.

Для беспроводных соединений используются различные технологии, такие как NFC, Wi-Fi, Bluetooth-соединения, UMTS, ANT, VSAT, ИК-соединения и т. д.

Такие сети отличаются простотой использования, синхронизацией, рентабельностью, достаточно высоким уровнем безопасности, автоматизированной настройкой и универсальностью.

Подвидом персональной сети можно назвать desk area network (DAN) – настольную рабочую сеть, т. е. сеть, образованную периферийными устройствами через рабочую станцию. Устройства взаимодействуют через ячейки асинхронной передачи данных. Режим асинхронной передачи данных означает, что данные передаются не непрерывным потоком, а отдельными пакетами. При этом указанный режим работает фактически как межсервисный провайдер.

Криминалистические аспекты сетей personal area network исследовались применительно к отдельным устройствам сети. Так, на настоящий момент имеют место публикации в области криминалистического исследования устройств Интернета вещей (IoT)[1], отдельных электронных гаджетов и устройств[2].

Между тем исследование общих вопросов данных сетей имеет непосредственное криминалистическое значение, поскольку позволяет установить факты вмешательства в сеть, использование сети для совершения преступления или отражения в ней криминалистически релевантной информации, связанной с событием преступления.

Тип и топология сети, количество и тип подключенных устройств, тип соединения, стандарт связи и скорость связи могут иметь криминалистическое значение одного из идентификаторов (цифрового отпечатка) сети или ее отдельных устройств и использования этого отпечатка для идентификации и аутентификации пользователей определенного ресурса или установления злоумышленников, использующих устройства сети для совершения преступлений.

При обнаружении в ходе следственных действий у сети personal area network описывается каждое устройство с точки зрения артикула, типа, модели, фирмы-произ-

[1] *Баяндурян А. К.* Использование специальных знаний при получении доказательственной информации из IoT-устройств // Цифровые технологии и право: сб. науч. тр. I Междунар. науч.-практ. конф., Казань, 23 сентября 2022 года / под ред. И. Р. Бегишева и др.: в 6 т. Т. 4. Казань: Познание, 2022. С. 59–62; *Смушкин А. Б.* Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460; *Servida F., Casey E.* IoT forensic challenges and opportunities for digital traces // Digital Investigation. Vol. 28. Supplement. April 2019. P. S22–S29 и др.

[2] *Мещеряков В. А., Яковлев А. Н.* «Электронная» составляющая осмотра места происшествия // Библиотека криминалиста. 2015. № 5; *Абдрахманова Л. Р., Аветисян К. Р.* Изучение возможности исследования «умных часов» для целей выявления противоправной деятельности // Прикладные исследования и технологии ART2019: сб. тр. регион. конф., Москва, 1–2 апреля 2019 года. М.: Московский технол. ин-т, 2019. С. 6–7; *Афонин О.* Криминалистический анализ часов Apple Watch S0, S1 и S2 // Блог Elcomsoft. URL: https://blog.elcomsoft.ru/2023/11/kriminalisticheskij-analiz-chasov-apple-watch-s0-s1-i-s2/ (дата обращения: 12.04.2024); *Seungjae Jeon, Jaehyun Chung, Doowon Jeong.* Watch Out! Smartwatches as criminal tool and digital forensic investigations. URL: https://arxiv.org/pdf/2308.09092v1.pdf (дата обращения: 12.04.2024) и др.

водителя, топологии подключения, состояния защиты, целевого предназначения и иных факторов.

В сетях любых видов исследуются информация о сетевом трафике, данные журналов (например, брандмауэра, коммутаторов и маршрутизаторов), сведения о попытках сетевых вторжений, информация, хранимая на устройствах сети.

Таким образом, проведенное исследование позволяет нам прийти к следующим выводам.

1. Перспективы развития этих сетей и их использования для управления объектами категории «Интернет вещей», компьютерного взлома и несанкционированного извлечения или модификации информации, внешнего криминального воздействия на те же элементы оздоровительной или мониторинговой нательной сети приводят к насущной необходимости разработки мер противодействия указанным действиям в целях обеспечения кибербезопасности.

2. Возможность использования этих сетей для несомненной идентификации человека, оценки действий в определенный момент времени, использование в качестве полиграфа также повышают важность криминалистических исследований в рассматриваемой области для правоохранительной деятельности, расследования преступлений, обеспечения личной безопасности и кибербезопасности граждан и юридических лиц.

3. Информация, извлекаемая из рассматриваемых сетей, может нести на себе следы внешнего вмешательства (взлома) нательной или персональной сети, отображать следы действий подозреваемого или потерпевшего до, в момент и после совершения преступления (как непосредственно с использованием данных сетей, так и являться виртуальным следом внешних по отношению к сети действий в системе сети BAN или PAN). Эта информация имеет несомненное криминалистическое значение. С учетом ее электронного характера она может быть использована в качестве электронных доказательств в различных видах судопроизводства.

4. Необходимо активизировать разработку технико-криминалистического и тактико-криминалистического обеспечения работы с рассматриваемыми видами сетей (как источника криминалистически значимой информации), определенный вклад в которую может внести и данная публикация. С технической точки зрения нуждаются в разработке новые приборы дистанционного выявления носителей сети и считывания отдельных ее параметров, аппаратно-программные комплексы работы с информацией сети и т. д. С тактической точки зрения необходимы разработки тактических рекомендаций по производству ОРМ и следственных действий, связанные с выявлением, фиксацией, изъятием и исследованием информации нательной и персональной сетей, сохранением фактора внезапности и возможностью дальнейшего использования информации в качестве доказательств.

5. Законодательное установление повышенной ответственности за причинение вреда здоровью человека или получение личной информации (например, о болезнях, генетических предрасположенностях и т. д.) при вмешательстве в нательную сеть путем дополнения соответствующих статей квалифицирующим признаком «с использованием компьютерных устройств» будет фактором общей и частной превенции.

6. Несомненно, данные, извлекаемые из сетей BAN и PAN, должны носить характер не только следственной тайны, но и (особенно в рамках гражданского, административного и арбитражного процессов) конфиденциальной информации, поскольку могут содержать не связанную с правонарушением информацию, которую лицо не хотело бы распространять (наличие определенных заболеваний, нахождение в определенном месте, конкретные виды активности и т. д.). Безопасность и конфиденциальность данных должны обеспечивать как способы их хранения и передачи, так и повышенная ответственность за их распространение.

Список литературы

Абдрахманова Л. Р., Аветисян К. Р. Изучение возможности исследования «умных часов» для целей выявления противоправной деятельности // Прикладные исследования и технологии ART2019: сб. тр. регион. конф., Москва, 1–2 апреля 2019 года. М.: Московский технол. ин-т, 2019. С. 6–7.

Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: моногр. М.: Юрлитинформ, 2012. 152 с.

Афонин О. Криминалистический анализ часов Apple Watch S0, S1 и S2 // Блог Elcomsoft. URL: https://blog.elcomsoft.ru/2023/11/kriminalisticheskij-analiz-chasov-apple-watch-s0-s1-i-s2/ (дата обращения: 12.04.2024).

Басов В. Хроники чипирования: как люди вживляют в себя микрочипы и можно ли сделать это незаметно // MAXIM. URL: https://www.maximonline.ru/lifestyle/khroniki-chipirovniya-kak-lyudi-vzhivlyayut-v-sebya-mikrochipy-i-mozhno-li-sdelat-eto-nezametno-id521598/ (дата обращения: 10.04.2024).

Баяндурян А. К. Использование специальных знаний при получении доказательственной информации из IoT-устройств // Цифровые технологии и право: сб. науч. тр. I Междунар. науч.-практ. конф., Казань, 23 сентября 2022 года / под ред. И. Р. Бегишева и др.: в 6 т. Т. 4. Казань: Познание, 2022. С. 59–62.

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

Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: моногр. Волгоград: ВА МВД России, 2008. 401 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: моногр. М.: Проспект, 2022. 176 с.

Мещеряков В. А., Яковлев А. Н. «Электронная» составляющая осмотра места происшествия // Библиотека криминалиста. 2015. № 5. С. 280–291.

Милашев В. А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: дис. … канд. юрид. наук. М., 2004. 208 с.

Нестеров А. В. Виртуальные следы в криминалистике: учеб. М.: КноРус, 2024. 153 с.

Смушкин А. Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460.

Смушкин А. Б. Цифровизация криминалистической деятельности: учеб. пособие / под ред. В. Б. Вехова. М.: КноРус, 2024. 198 с.

Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков; под ред. Е. Р. Россинской; Министерство науки и высшего образования Российской Федерации; Московский гос. юрид. ун-т им. О. Е. Кутафина (МГЮА). М.: Проспект, 2022. С. 256 с.

Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юрид. мир, 2007. 418 с.

Цифровые следы преступлений: моногр. М.: Проспект, 2021. 168 с.

Яковлев А. Н. Теоретические и методические основы экспертного исследования документов на машинных носителях информации: дис. … канд. юрид. наук. Саратов, 2000. 218 с.

Bella V. Chinese brain chip helps paralysed man regain mobility – and it's less invasive than Elon Musk's Neuralink // South China Morning Post. URL: https://www.scmp.com/news/china/science/article/3250476/chinese-brain-chip-helps-paralysed-man-regain-mobility-and-its-less-invasive-elon-musks-neuralink?module=top_story&pgtype=homepage (дата обращения: 10.04.2024).

Grauer Y. A practical guide to microchip implants // ARSTECHNICA. URL: https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/ (дата обращения: 10.04.2024).

Servida F., Casey E. IoT forensic challenges and opportunities for digital traces // Digital Investigation. Vol. 28. Supplement. April 2019. P. S22–S29.

Seungjae Jeon, Jaehyun Chung, Doowon Jeong. Watch Out! Smartwatches as criminal tool and digital forensic investigations. URL: https://arxiv.org/pdf/2308.09092v1.pdf (дата обращения: 12.04.2024).

References

Abdrakhmanova L. R., Avetisyan K. R. (2019) Izuchenie vozmozhnosti issledovaniya «umnykh chasov» dlya tselei vyyavleniya protivopravnoi deyatel'nosti [Exploring the possibility of researching «smart watches» for the purpose of identifying illegal activitie]. In *Prikladnye issledovaniya i tekhnologii ART2019: conference papers*. Moscow, Moskovskii tekhnologicheskii institut, pp. 6–7.

Afonin O. (2023) Kriminalisticheskii analiz chasov Apple Watch S0, S1 i S2 [Forensic analysis of Apple Watch S0, S1 and S2]. In *Blog Elcomsoft*, available at: blog.elcomsoft.ru/2023/11/kriminalisticheskij-analiz-chasov-apple-watch-s0-s1-i-s2/ (accessed: 12.04.2024).

Agibalov V. Yu. (2012) *Virtual'nye sledy v kriminalistike i ugolovnom protsesse: monografiya* [Virtual traces in criminalistics and criminal procedure: monography]. Moscow, Yurlitinform, 152 p.

Basov V. (2020) Khroniki chipirovaniya: kak lyudi vzhivlyayut v sebya mikrochipy i mozhno li sdelat' eto nezametno [Chronicles of chipping: how do people implant microchips into themselves and is it

possible to do it unnoticeably]. In *MAXIM*, available at: https://www.maximonline.ru/lifestyle/khroniki-chipirovniya-kak-lyudi-vzhivlyayut-v-sebya-mikrochipy-i-mozhno-li-sdelat-eto-nezametno-id521598/ (accessed: 10.04.2024).

Bayanduryan A. K. (2022) Ispol'zovanie spetsial'nykh znanii pri poluchenii dokazatel'stvennoi informatsii iz IoT-ustroistv [The use of special knowledge in obtaining evidentiary information from IoT devices]. In *Tsifrovye tekhnologii i pravo: conference papers*, ed. by I. R. Begishev, etc.: in 6 volumes. Vol. 4. Kazan', Poznanie, pp. 59–62.

Bella V. Chinese brain chip helps paralysed man regain mobility – and it's less invasive than Elon Musk's Neuralink. In *South China Morning Post*, available at: https://www.scmp.com/news/china/science/article/3250476/chinese-brain-chip-helps-paralysed-man-regain-mobility-and-its-less-invasive-elon-musks-neuralink?module=top_story&pgtype=homepage (accessed: 10.04.2024).

Fedotov N. N. (2007) *Forenzika – komp'yuternaya kriminalistika* [Forenzika – computer criminalistics]. Moscow, Yuridicheskii mir, 418 p.

Grauer Y. (2018) A practical guide to microchip implants. In *ARSTECHNICA*, available at: https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/ (accessed: 10.04.2024).

Meshcheryakov V. A. (2001) *Osnovy metodiki rassledovaniya prestuplenii v sfere komp'yuternoi informatsii: dis. … d-ra yurid. nauk* [Fundamentals of the methodology for investigating crimes in the field of computer information: a doctor of legal sciences thesis]. Voronezh, 387 p.

Meshcheryakov V. A. (2022) *Teoreticheskie osnovy mekhanizma sledoobrazovaniya v tsifrovoi kriminalistike: monografiya* [Theoretical foundations of the mechanism of trace formation in digital forensics: a monography]. Moscow, Prospekt, 176 p.

Meshcheryakov V. A., Yakovlev A. N. (2015) «Elektronnaya» sostavlyayushchaya osmotra mesta proisshestviya [«Electronic» component of the inspection of the scene of the incident]. In *Biblioteka kriminalista*, no. 5, pp. 280–291.

Milashev V. A. (2004) *Problemy taktiki poiska, fiksatsii i iz"yatiya sledov pri nepravomernom dostupe k komp'yuternoi informatsii v setyakh EVM: dis. … kand. yurid. nauk* [Problems of tactics of search, fixation and removal of traces in case of unauthorized access to computer information in computer networks: a candidate of legal sciences thesis]. Moscow, 208 p.

Nesterov A. V. (2024) *Virtual'nye sledy v kriminalistike: uchebnik* [Virtual traces in criminalistics: textbook]. Moscow, KnoRus, 153 p.

Rossinskaya E. R. (Ed.) (2022) *Teoriya informatsionno-komp'yuternogo obespecheniya kriminalisticheskoi deyatel'nosti* [Theory of information and computer support for forensic activities]. Moscow, Prospekt, 256 p.

Servida F., Casey E. (2019) IoT forensic challenges and opportunities for digital traces. In *Digital Investigation*, vol. 28, Supplement, April, pp. 22–29.

Seungjae Jeon, Jaehyun Chung, Doowon Jeong (2023) *Watch Out! Smartwatches as criminal tool and digital forensic investigations*, available at: https://arxiv.org/pdf/2308.09092v1.pdf (accessed: 12.04.2024).

Smushkin A. B. (2020) Otdel'nye aspekty ispol'zovaniya kontseptsii interneta veshchei v tselyakh protivodeistviya prestupnosti [Certain aspects of using the concept of the Internet of Things in order to counter crime]. In *Vserossiiskii kriminologicheskii zhurnal*, vol. 14, no. 3, pp. 453–460, DOI: 10.17150/2500-4255.2020.14(3).453-460.

Smushkin A. B. (2024) *Tsifrovizatsiya kriminalisticheskoi deyatel'nosti: uchebnoe posobie* [Digitalization of criminalistic activity: textbook], ed. by V. B. Vekhov. Moscow, KnoRus, 198 p.

Tsifrovye sledy prestuplenii: monografiya (2021) [Digital traces of crimes: monography]. Moscow, Prospekt, 168 p.

Vekhov V. B. (2008) *Kriminalisticheskoe uchenie o komp'yuternoi informatsii i sredstvakh ee obrabotki: avtoref. dis. … d-ra yurid. nauk* [Criminalistic doctrine of computer information and means of its processing: an abstract of a doctor of legal sciences thesis]. Volgograd, 45 p.

Vekhov V. B. (2008) *Osnovy kriminalisticheskogo ucheniya ob issledovanii i ispol'zovanii komp'yuternoi informatsii i sredstv ee obrabotki: monografiya* [Fundamentals of criminalistic teaching on the study and use of computer information and its processing tools: monography]. Volgograd, VA MVD Rossii, 401 p.

Yakovlev A. N. (2000) *Teoreticheskie i metodicheskie osnovy ekspertnogo issledovaniya dokumentov na mashinnykh nositelyakh informatsii: dis. … kand. yurid. nauk* [Theoretical and methodological foundations of expert research of documents on machine media: a candidate of legal sciences thesis]. Saratov, 218 p.

Дата поступления рукописи в редакцию: 17.10.2024
Дата принятия рукописи в печать: 20.02.2025