DOI: 10.17803/1994-1471.2025.171.2.125-133

А. В. Коринь*

Интернет вещей: криминалистические аспекты

Аннотация. В работе представлен обзор криминальных угроз в области эксплуатации умных устройств (IoT-устройств). Особое внимание уделено использованию ботнетов из скомпрометированных умных устройств для совершения DDoS-атак, распространения вредоносного программного обеспечения, майнинга криптовалюты, превращения умных устройств в прокси-серверы. Автором рассмотрены основные факторы уязвимости умных устройств. Сделан вывод о том, что IoT-устройства являются ценными источниками криминалистически значимой информации, в первую очередь о пространственно-временны́х факторах. Отмечена возможность использования умных устройств в целях противодействия расследованию преступлений. Автор обращает внимание на целесообразность привлечения специалиста для работы с умными устройствами в ходе следственных действий, т.к. умные устройства являются носителями цифровых следов. Подчеркивается важность подготовительного этапа в проведении следственных действий, предполагающих работу с умными устройствами. Сформулирован алгоритм поэтапной проверки криминалистически значимой информации, полученной от умных устройств.

Ключевые слова: интернет вещей (IoT); умные устройства (IoT-устройства); ботнет; DDoS-атака; вредоносное программное обеспечение; цифровой след; специалист; криминалистически значимая информация; пространственно-временны́е факторы; судебная компьютерно-техническая экспертиза.

Для цитирования: *Коринь А. В.* Интернет вещей: криминалистические аспекты // Актуальные проблемы российского права. — 2025. — Т. 20. — № 2. — С. 125–133. — DOI: 10.17803/1994-1471.2025.171.2.125-133.

Internet of Things: Forensic Aspects

Aleksey V. Korin, Postgraduate Student, Department of Criminalistics, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
korin.alexej@yandex.ru

Abstract. The paper presents an overview of criminal threats in the field of exploitation of smart devices (IoT devices). Particular attention is given to the use of botnets of compromised smart devices to carry out DDoS attacks, distribute malware, mine cryptocurrency, and turn smart devices into proxy servers. The author examines the main factors that determine the vulnerability of smart devices. It is concluded that IoT devices are valuable sources of forensically significant information, primarily information about spatio-temporal factors. The possibility of using smart devices to counteract crime investigations was noted. The author draws attention to the advisability of involving a specialist to work with smart devices during investigative actions, since smart devices are carriers of digital traces. The importance of the preparatory stage in conducting investigative actions that involve working with smart devices is emphasized. An algorithm for the step-by-step verification of forensically significant information obtained from smart devices has been formulated.

* *Коринь Алексей Вячеславович*, соискатель кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Российская Федерация, 125993
korin.alexej@yandex.ru

Keywords: Internet of Things (IoT); smart devices (IoT devices); botnet; DDoS attack; malware; digital footprint; specialist; forensically significant information; spatio-temporal factors; forensic computer expertise.
Cite as: Korin AV. Internet of Things: Forensic Aspects. *Aktual'nye problemy rossijskogo prava*. 2025;20(2):125-133. (In Russ.). DOI: 10.17803/1994-1471.2025.171.2.125-133.

В настоящее время возросло применение интернета вещей во всех сферах жизнедеятельности человека. Впервые термин «интернет вещей» (Internet of Things, IoT) был введен в оборот в 1999 г. основателем исследовательской группы Auto-ID при Массачусетском технологическом институте Кевином Эштоном[1]. С тех пор термин прочно вошел в повседневный лексикон и, согласно одному из наиболее популярных определений, означает «динамическую глобальную сетевую инфраструктуру с возможностями самоконфигурирования на основе стандартных и совместимых протоколов связи, где физические и виртуальные "вещи" имеют идентификаторы, физические и виртуальные атрибуты и используют интеллектуальные интерфейсы, а также легко интегрируются в инфокоммуникационные технологии и информационную сеть»[2].

На сегодняшний день можно с полной уверенностью утверждать о состоявшемся переходе от интернета людей к интернету вещей. По данным статистического портала «Statista», количество вещей, подключенных к сети Интернет, по всему миру в 2021 г. достигло 11,3 млрд с перспективой увеличения до более чем 29 млрд устройств интернета вещей в 2030 г.[3] Аналитики корпорации «Cisco» считают период с 2008 по 2009 г. настоящим рождением интернета вещей, т.к. именно в этом промежутке количество устройств, подключенных к глобальной сети, превысило численность населения Земли[4]. Однако, по нашему мнению, на тот момент технологии интернета вещей еще не достигли зрелости: умные вещи имели ограниченное распространение, в основном представляли собой смартфоны, роутеры и видеокамеры. В настоящий момент устройства интернета вещей (далее — умные или IoT-устройства) применяются в здравоохранении, промышленности, военно-промышленном комплексе, сельском хозяйстве, ритейле, участвуют в управлении жизнью города («умный город») и стали привычными атрибутами окружающего мира, воспринимаются как нечто само собой разумеющееся (например, устройства «умного дома»: датчики открытия дверей и окон, датчики дыма, камеры видеонаблюдения, лампочки, системы вентиляции, метеодатчики, счетчики электричества, воды, отопления и т.д.).

По нашему мнению, маркером перехода от интернета людей к интернету вещей является не превышение количеством умных устройств числа людей, а создание и развитие нового вида социальной связи «вещь — вещь».

Говоря о ценности интернета вещей, необходимо принимать во внимание эффект эммерджентности — появление у громадного количества умных устройств, объединенных в единую систему, новых качеств. Концепция интернета вещей позволяет не только объединять предметы материального мира посредством Интернета для обмена информацией между ними, но и развивать возможности накопления, структурирования и анализа различной информации.

---

1 *Черняк Л. С.* Платформа интернета вещей // Открытые системы. СУБД. 2012. № 7. С. 44.

2 *Жариков А. Р.* Перспективы развития и правовое регулирование индустриального интернета вещей в России // Вопросы современной науки и практики. Университет имени В.И. Вернадского. 2018. № 2 (68). С. 106.

3 Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 // URL: http://https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (дата обращения: 21.03.2024).

4 *Evans D.* The Internet of Things. How the Next Evolution of the Internet Is Changing Everything (April 11, 2011) // URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (дата обращения: 21.03.2024).

Ценность интернета вещей осознает в полной мере и преступный мир, в орбиту интересов которого всё чаще попадают умные устройства. Как правильно отмечают ученые, «современные научные открытия и технические достижения открывают широкие перспективы для социально-экономического и культурного прогресса, но они могут поставить под угрозу и осуществление прав и свобод человека»[5].

Чем привлекательны IoT-устройства для преступников?

1. Эти устройства являются ценными источниками информации о своем владельце. Так, смартфон, умные часы, браслеты, весы способны поведать о состоянии здоровья человека. Данные видеокамер, умных колонок, датчиков движения и освещения расскажут о его передвижениях, привычках и увлечениях. Не менее ценными являются и хранящиеся в умных устройствах данные банковских карт для покупок в онлайн-магазинах, логины и пароли для соцсетей, переписка в соцсетях, электронной почте и пр.

В следственной практике всё чаще встречаются примеры использования злоумышленниками данной информации для подготовки, совершения и сокрытия преступлений. Так, житель г. Черкесска, являясь сотрудником IT-компании, используя служебное положение, получил доступ к личному кабинету приложения «умный дом» двух жительниц Черкесска и осуществлял просмотры видеокамер, установленных в квартирах потерпевших. В дальнейшем данный гражданин был задержан сотрудниками полиции, в отношении него было возбуждено два уголовных дела[6].

2. Взлом умных устройств позволяет преступникам строить из них ботнеты. М. Ю. Косенко и А. В. Мельников приводят следующее определение: ботнет — это сеть ботов, которые находятся под удаленным контролем злоумышленника. Бот — программное обеспечение робота, экземпляр вредоносного программного обеспечения, работающий на зараженном компьютере автономно и автоматически без ведома пользователя[7].

Полагаем, что в современных реалиях данное определение нуждается в корректировке, т.к. частью ботнета может стать не только компьютер, но и иное компьютерное устройство. В этой связи уместно обратить внимание на позицию Верховного Суда РФ, изложенную в постановлении Пленума от 15.12.2022 № 37: «К числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом»[8]. Исходя из изложенного, допустимо отнесение IoT-устройств к числу компьютерных устройств.

Рассмотрим основные способы использования ботнетов в преступной деятельности.

---

[5] *Ищенко Е. П.*, *Кручинина Н. В.* Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. 2022. № 2. С. 199.

[6] В Карачаево-Черкесии работник IT-компании подозревается в получении неправомерного доступа к компьютерной информации // URL: https://09.мвд.рф/news/item/28097143 (дата обращения: 01.04.2024).

[7] *Косенко М. Ю.*, *Мельников А. В.* Вопросы обеспечения защиты информационных систем от ботнет атак // Вопросы кибербезопасности. 2016. № 4 (17). С. 20.

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

2.1. Ботнет используется для совершения DDoS-атак (Distributed Denial of Service, или «распределенный отказ в обслуживании»). Атака «отказ в обслуживании» — сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе[9]. Суть данной атаки заключается в том, что с ботнета на веб-сервер направляется огромное число ложных, пустых запросов, превышающее пропускные возможности канала связи или возможности по одновременной обработке запросов веб-сервером. В результате этих действий появляются перебои в работе или происходит падение сайта, потому что его веб-сервер начинает испытывать перегрузку и не может своевременно обрабатывать легитимные запросы.

Известна DDoS-атака на веб-серверы американского интернет-провайдера Dyn, в результате которой в течение нескольких часов было недоступно более 80 интернет-платформ по всему миру, среди которых Netflix, Amazon, Airbnb, GitHub, HBO, CNN и др. По данным «Лаборатории Касперского», атака на Dyn проводилась с помощью гигантского ботнета, включавшего десятки миллионов устройств: IP-камеры, роутеры, принтеры и другие устройства из интернета вещей. Все вместе они передавали данные на серверы Dyn со скоростью 1,2 Тбит/с[10].

В основном DDoS-атаки используются в качестве инструмента для совершения следующих видов преступлений:

— вымогательство за остановку атаки. Требование выплаты вознаграждения в криптовалюте зачастую позволяет сохранить анонимность преступника;

— воздействие на критическую информационную инфраструктуру Российской Федерации. Всё чаще в качестве целей преступники выбирают объекты критической инфраструктуры: объекты энергетики, медицинские учреждения, сайты государственных органов и Единый портал государственных и муниципальных услуг, систему дистанционного электронного голосования в ходе выборов и пр.;

— DDoS-атака как попытка воспрепятствования функционированию бизнеса конкурента. Остановка/замедление работы сайта, нарушение процессов продаж, обслуживания, информирования могут дискредитировать или разрушить бизнес;

— с целью сокрытия других преступлений или облегчения их совершения, например, чтобы отвлечь внимание от проникновения в инфраструктуру организации или вывести уже полученную информацию;

— DDoS-атаки применяются и активистами, стремящимися с помощью кибератак обратить внимание общественности на социальные, политические и другие проблемы. Данное явление получило название «хактивизм» (от англ. hacktivizm).

2.2. На входящие в ботнет скомпрометированные устройства может быть загружено вредоносное программное обеспечение с целью сбора личной информации о владельце, рассылки спама или распространения вредоносного программного обеспечения. Например, по приговору суда М. был осужден по ч. 1 ст. 273 УК РФ[11]. Согласно установленным по делу обстоятельствам, М. использовал вредоносное программное обеспечение для заражения 50 ЭВМ неустановленных пользователей сети Интернет и построения на их основе ботнета, предназначенного для несанкционированного копирования информации о логинах и паролях

[9] Национальный стандарт ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 01.10.2009 (ред. от 01.11.2018) // СПС «Кодекс».

[10] Что случилось с Twitter, PayPal, Amazon и другими американскими сервисами // URL: https://www.kaspersky.ru/blog/attack-on-dyn-explained/13471/ (дата обращения: 02.04.2024).

[11] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 23.03.2024) // СПС «КонсультантПлюс».

[12] Приговор Андроповского районного суда Ставропольского края от 06.04.2017 № 1-31/2017 по делу № 1-31/2017 // URL: https://sudact.ru/regular/doc/EkNTBHRi14x1/?regular-txt=ботнет&regular-case_

авторизации пользователей на различных интернет-ресурсах[12].

2.3. Вычислительные мощности устройств, составляющих ботнет, могут быть использованы для майнинга криптовалюты.

2.4. Устройства могут быть превращены в прокси-серверы, которые используются для перенаправления сетевого трафика преступников, при этом затрудняется его отслеживание и обеспечивается анонимность преступника. Зачастую созданные таким образом прокси-серверы сдаются в аренду другим преступникам. Так, по приговору суда П. был осужден по ч. 1 ст. 273 УК РФ. Согласно установленным по делу обстоятельствам, П. использовал вредоносное программное обеспечение для получения доступа к удаленным компьютерам, создания ботнета из роутеров и использования их в качестве прокси-сервера[13].

Развитие и повсеместное распространение технологии интернета вещей открыло перед преступным миром множество возможностей для использования в своих целях IoT-устройств. Полагаем, что высокая уязвимость умных устройств обусловлена рядом факторов, среди которых необходимо выделить следующие:

— производители умных устройств по-прежнему действуют как обычные производители бытовой техники и электроники, а не как поставщики цифровых услуг. Следствие — уязвимости на аппаратном уровне или на уровне программного обеспечения производимых устройств, медленная реакция производителей на выявленные уязвимости в их продуктах (несвоевременный выпуск обновлений программного обеспечения или их полное отсутствие);

— проблема совместимости умных устройств от разных производителей. При построении системы «умного дома» редко используется оборудование одного производителя, что приводит к конфликту протоколов обмена данными (например, некорректная реализация защищенного соединения между двумя устройствами влечет за собой угрозу перехвата данных);

— передача данных между устройством и облачным хранилищем создает риск их перехвата;

— несоблюдение пользователями умных устройств базовых правил информационной безопасности (использование заводских паролей, предоставление доступа к домашней сети Wi-Fi посторонним лицам, отказ от обновления программного обеспечения и пр.).

С другой стороны, насыщение окружающей среды умными устройствами привело к тому, что они всё чаще встречаются в обстановке совершения преступления. Данное обстоятельство необходимо учитывать следователям, особенно при производстве таких следственных действий, как осмотр и обыск. Предназначенные для сбора информации и обмена ею умные устройства являются ценными источниками криминалистически значимой информации.

По содержанию это преимущественно информация о пространственно-временны́х факторах. Так, наиболее полную информацию о передвижениях конкретного лица умные устройства (смартфоны, часы, браслеты) способны дать благодаря приемнику GPS, которым оснащены большинство из них. Если устройства привязаны к смартфону, то через него можно установить их нахождение. Также информацией о факте передвижения лица, пройденном расстоянии, скорости передвижения устройства могут поделиться благодаря наличию функции подсчета пройденных шагов (шагомера). Информацию о передвижениях лица, факте его нахождения/отсутствия в помещении можно получить в результате анализа данных различных датчиков: открытия окон и дверей, освещенности, движения.

Подавляющее большинство устройств ведут журнал активности, в котором фиксируются факты использования устройства, продолжительность выполнения отдельных действий.

doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1665089289280 (дата обращения: 02.04.2024).

[13] Приговор Октябрьского районного суда г. Новосибирска от 23.12.2016 по делу № 1-584/2016 // URL: https://actofact.ru/case-54RS0007-1-584-2016-2016-10-06-2-0/ (дата обращения: 02.04.2024).

Умная колонка способна сообщить, в течение какого времени она работала. Умная подушка фиксирует время сна, в том числе моменты пробуждения и засыпания. Часы и браслеты самостоятельно определяют виды физической активности, фиксируют их продолжительность.

Информацию о состоянии здоровья человека (пульс, уровень кислорода в крови, артериальное давление, уровень стресса и пр.), его антропометрических характеристиках собирают такие IoT-устройства, как весы, зубная щетка, фитнес-браслет, часы и, конечно же, смартфон, в котором, как правило, объединяется вся эта информация. Эти данные могут быть приняты во внимание при решении вопроса о нахождении лица в необычном психофизиологическом состоянии.

Синхронизированные со смартфоном умные часы и фитнес-браслеты могут содержать историю звонков, посещения сайтов в сети Интернет; данные банковских карт; переписку в мессенджерах и социальных сетях, электронной почте; фото-, видео- и аудиозаписи. Последние могут быть сделаны и самим умным устройством, оснащенным видеокамерой.

О привычках, распорядке дня человека могут рассказать журналы активности умных вещей, установленные сценарии. Сценарий — набор команд, последовательность действий, которую пользователь устанавливает в контроллере «умного дома» для умных устройств.

Вместе с тем необходимо учитывать возможность использования преступником умных устройств для создания ложного алиби, инсценировки события преступления. В частности, злоумышленник с помощью смартфона, который работает как управляющий элемент для системы «умный дом», может удаленно запустить один из сценариев, цель которых — создать видимость его присутствия в доме. По определенному сигналу в доме автоматически включится свет, закроются шторы на окнах и умная колонка начнет воспроизводить музыку — это создаст у соседей впечатление, что он действительно там находится.

Уместно обратить внимание на зарубежный опыт использования IoT-устройств при раскрытии и расследовании преступлений. В США известен случай, когда данные фитнес-браслета помогли опровергнуть ложные показания потерпевшей по делу об изнасиловании. Анализ данных гаджета показал, что потерпевшая не спала, а ходила по дому, что противоречило ее показаниям[14]. По другому делу фитнес-браслет зафиксировал изменения пульса убитой женщины: ее сердцебиение резко замедлилось и остановилось в 15:28, примерно за пять минут до того, как подозреваемый, судя по данным наружных камер видеонаблюдения, покинул дом жертвы[15]. Аналогичное дело было раскрыто в Греции, где данные умных часов и смартфона обратили внимание следствия на несоответствия в показаниях подозреваемого. Так, согласно данным шагомера, установленного на смартфоне подозреваемого, он был активен в тот момент, когда, по его утверждению, он был обездвижен грабителями[16].

Таким образом, криминалистически значимая информация, которую аккумулируют в себе умные устройства, может быть использована для разрешения целого ряда задач, возникающих на этапе предварительного расследования, в первую очередь таких, как установление базовых элементов события преступления: времени и места; проверка алиби подозреваемого; выявление и разоблачение инсценировки; преодоление ложных показаний (в том числе самооговора).

Впрочем, собирание данной информации — задача не из легких. Работа с умными устройствами, обнаруженными на месте происшествия либо в ходе обыска, имеет специфику, которую

[14] Woman's FitBit watch disproves her rape story // URL: https://www.reviewjournal.com/uncategorized/womans-fitbit-watch-disproves-her-rape-story/ (дата обращения: 03.04.2024).

[15] Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing // URL: https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html (дата обращения: 03.04.2024).

[16] How app and fitness watch helped convict Brit mum Caroline Crouch's husband killer // URL: https://www.mirror.co.uk/news/world-news/how-app-fitness-watch-helped-26986593 (дата обращения: 03.04.2024).

необходимо учитывать следователю: умные устройства являются носителями цифровых следов — криминалистически значимой компьютерной информации о событиях/действиях в процессе ее возникновения, обработки, хранения, передачи, отраженной в материальной среде[17].

Одним из свойств цифровых следов является возможность их быстрого уничтожения или преобразования в другую форму, что может привести к утрате криминалистически значимой информации. Поэтому при работе с умными устройствами должна быть обеспечена неизменность хранящихся в них цифровых следов. Достигается это путем применения криминалистических программных и аппаратных средств (копировщиков и блокираторов). Кроме того, в протоколе следственного действия в полном объеме должны быть зафиксированы все действия по изъятию, хранению и передаче цифровых следов, доступу к ним и, соответственно, к устройствам, на которых они содержатся.

Для работы с умными устройствами в ходе следственных действий рекомендуется привлекать специалиста, имеющего соответствующую подготовку. Это особенно важно ввиду того, что большинство преступлений, совершенных с использованием IoT-устройств, совершается в условиях неочевидности, когда потерпевший сталкивается с наступившими в результате совершенного деяния негативными последствиями, но ни способ преступления, ни преступник неизвестны.

Специалист может обратить внимание следователя на необходимость исследования умных устройств, которые хотя и не были непосредственно использованы при совершении преступления, но хранящаяся на них информация может быть полезна для установления обстоятельств, имеющих значение для уголовного дела.

В случае необходимости изъятия умного устройства в ходе производства следственных действий частью 2 ст. 164.1 УПК РФ[18] прямо предусмотрено обязательное участие специалиста.

В том случае, если специалисту не удается извлечь цифровые следы из умного устройства, то в отношении устройства необходимо назначить судебную компьютерно-техническую экспертизу. К слову, в научной литературе давно высказывается мнение о необходимости выделения такого рода судебной компьютерно-технической экспертизы, как экспертиза нетипичных компьютерных средств, и ее видов: программно-компьютерной экспертизы нетипичных компьютерных средств, информационно-компьютерной экспертизы нетипичных компьютерных средств[19].

Специалист еще на этапе подготовки к производству следственного действия в зависимости от конкретных обстоятельств дела должен оказать содействие следователю в разработке плана следственного действия, обратить внимание на технические возможности умных устройств, предусмотреть порядок действий на месте, рассмотреть возможные проблемные ситуации, связанные с поиском, фиксацией и изъятием умных устройств и хранящихся на них цифровых следов, и способы их разрешения.

Проверка криминалистически значимой информации, полученной от умных устройств, должна осуществляться в несколько этапов.

На первом этапе при помощи специалиста следователь должен проанализировать данные, полученные от умных устройств, на предмет их соответствия стандартам точности и надежности. Во внимание должны быть приняты точность и погрешность измерений, производимых

---

[17] *Россинская Е. Р., Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 8.

[18] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 23.03.2024) // СПС «КонсультантПлюс».

[19] Судебная экспертиза в цивилистических процессах : науч.-практ. пособие / под ред. Е. Р. Россинской. М. : Проспект, 2018. С. 316.

устройствами. Необходимо удостовериться, что устройство вело записи надлежащим образом. Погрешности, аномалии в данных могут возникать из-за ошибок в работе устройств, проблем с подключением, потери сигнала или неправильной калибровки датчиков. Также нельзя игнорировать вероятность того, что данные, хранящиеся в умных устройствах, были ранее фальсифицированы.

На втором этапе целесообразно сопоставление данных из разных умных устройств, собирающих аналогичную информацию. Например, умные часы и фитнес-браслеты собирают сведения о геопозиционировании устройства, раскрывающие местонахождение его пользователя в конкретный период. Эти данные могут быть сопоставлены с данными, полученными с других устройств, таких как смартфоны или планшеты, которые также собирают аналогичную информацию.

Третий этап заключается в сопоставлении данных умных устройств с криминалистически значимой информацией, полученной из иных источников. Так, в результате допроса свидетелей может быть установлено, что в день совершения преступления подозреваемый отдал во временное пользование умные часы другому лицу, что опровергает показания подозреваемого о нахождении в другом месте во время совершения преступления.

Необходимо добавить, что за деятельностью по проверке криминалистически значимой информации следует (а зачастую сопутствует ей) деятельность, направленная на оценку данного вида информации[20].

Резюмируя вышесказанное, отметим, что стремительное распространение умных устройств повлекло за собой возникновение новых криминальных угроз, что ставит большие задачи перед криминалистической наукой. Вместе с тем IoT-устройства являются ценными источниками различной криминалистически значимой информации, и в первую очередь о пространственно-временны́х факторах. Работа с умными устройствами в ходе производства следственных действий требует от следователя знания правил работы с цифровыми следами и в большинстве случаев предполагает участие специалиста. Следует еще раз подчеркнуть важность подготовительного этапа в проведении следственных действий, предполагающих работу с умными устройствами.

БИБЛИОГРАФИЯ

1. *Жариков А. Р.* Перспективы развития и правовое регулирование индустриального интернета вещей в России // Вопросы современной науки и практики. Университет имени В.И. Вернадского. — 2018. — № 2 (68). — С. 105–113.
2. *Ищенко Е. П.*, *Кручинина Н. В.* Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. — 2022. — № 2. — С. 199–206.
3. *Коринь А. В.* Проблемы проверки криминалистически значимой информации // Советская и российская криминалистика: традиции и перспективы : материалы Всероссийской научно-практической конференции с международным участием, Москва, 2 февраля 2023 г. — М. : Московская академия Следственного комитета Российской Федерации, 2023. — С. 95–97.
4. *Косенко М. Ю.* Вопросы обеспечения защиты информационных систем от ботнет атак // Вопросы кибербезопасности. — 2016. — № 4 (17). — С. 20–28.
5. *Россинская Е. Р.*, *Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции, Алматы, 19 февраля 2019 г. —

[20] *Коринь А. В.* Проблемы проверки криминалистически значимой информации // Советская и российская криминалистика: традиции и перспективы : материалы Всероссийской научно-практической конференции с международным участием, Москва, 2 февраля 2023 г. М. : Московская академия Следственного комитета РФ, 2023. С. 97.

Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖ¥Б, 2019. — С. 6–9.
6. Судебная экспертиза в цивилистических процессах : науч.-практ. пособие / под ред. Е. Р. Россинской. — М. : Проспект, 2018. — 704 с.
7. *Черняк Л. С.* Платформа интернета вещей // Открытые системы. СУБД. — 2012. — № 7. — С. 44–45.

Материал поступил в редакцию 11 апреля 2024 г.

REFERENCES (TRANSLITERATION)

1. Zharikov A. R. Perspektivy razvitiya i pravovoe regulirovanie industrialnogo interneta veshchey v Rossii // Voprosy sovremennoy nauki i praktiki. Universitet imeni V.I. Vernadskogo. — 2018. — № 2 (68). — S. 105–113.
2. Ishchenko E. P., Kruchinina N. V. Vysokie tekhnologii i kriminalnye vyzovy // Vserossiyskiy kriminologicheskiy zhurnal. — 2022. — № 2. — S. 199–206.
3. Korin A. V. Problemy proverki kriminalisticheski znachimoy informatsii // Sovetskaya i rossiyskaya kriminalistika: traditsii i perspektivy: materialy Vserossiyskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem, Moskva, 2 fevralya 2023 g. — M.: Moskovskaya akademiya Sledstvennogo komiteta Rossiyskoy Federatsii, 2023. — S. 95–97.
4. Kosenko M. Yu. Voprosy obespecheniya zashchity informatsionnykh sistem ot botnet atak // Voprosy kiberbezopasnosti. — 2016. — № 4 (17). — S. 20–28.
5. Rossinskaya E. R., Ryadovskiy I. A. Kontseptsiya tsifrovykh sledov v kriminalistike // Aubakirovskie chteniya: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii, Almaty, 19 fevralya 2019 g. — Almaty: Қazaқstan Respublikasy IIM M. Esbolatov atyndaғy Almaty akademiyasyның ҒZzhRBZh¥B, 2019. — S. 6–9.
6. Sudebnaya ekspertiza v tsivilisticheskikh protsessakh: nauch.-prakt. posobie / pod red. E. R. Rossinskoy. — M.: Prospekt, 2018. — 704 s.
7. Chernyak L. S. Platforma interneta veshchey // Otkrytye sistemy. SUBD. — 2012. — № 7. — S. 44–45.