ISSN 2500-4255

УДК 343.98
DOI 10.17150/2500-4255.2020.14(3).453-460

ОТДЕЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОНЦЕПЦИИ ИНТЕРНЕТА ВЕЩЕЙ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

А.Б. Смушкин[1, 2]
[1] Саратовская государственная юридическая академия, г. Саратов, Российская Федерация
[2] Поволжский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), г. Саратов, Российская Федерация

Информация о статье

Дата поступления
22 августа 2019 г.

Дата принятия в печать
25 июня 2020 г.

Дата онлайн-размещения
30 июня 2020 г.

Ключевые слова
Интернет вещей; умный дом; умный автомобиль; умные часы; криминалистическое исследование; электронные доказательства; электронные цифровые следы

Аннотация. В статье констатируется наступление эры интернета вещей. Отмечается, что в отечественной юридической литературе уделяется недостаточное внимание практическим вопросам правоприменения, возникающим в ходе реализации концепции интернета вещей, в частности криминалистическому исследованию и использованию умных вещей правоохранительными органами. Общий криминалистический анализ реализации концепции интернета вещей в отечественной научной литературе проводится впервые. Рассматривая практическое воплощение указанной концепции, автор приходит к выводу о необходимости не просто выделения умного дома, умного автомобиля и умных вещей, но объединения их в единую систему умной среды обитания. Отмечается, что элементы, относящиеся к публичной сфере применения интернета вещей, заслуживают отдельных исследований, а в фокусе внимания данной статьи будет только бытовое применение. Выявляются современные препятствия к полномасштабной реализации интернета вещей. Проведение криминалистического исследования интернета вещей и умной среды обитания позволяет определить основные системы, которые составляет современная техника в рассматриваемой сфере, и требования к ним, подсистемы умного дома, функции умных автомобилей и гаджетов. Констатируется, что криминалистическое исследование подсистем умной среды обитания возможно с помощью научных криминалистических разработок в области электронных цифровых следов и электронных доказательств. Установлены основные точки поиска этих следов. В статье последовательно рассмотрено, какая криминалистически значимая информация может быть получена при изучении датчиков и памяти умных вещей, умного автомобиля и умного дома. Определены функции, анализ которых имеет большое значение для сбора доказательственной и ориентирующей информации. Утверждается, что вся передаваемая от датчиков всех устройств информация в итоге аккумулируется в центре управления, а также на серверах облачных и сетевых сервисов, предназначенных для работы интернета вещей. Подчеркивается, что все действия с электронными цифровыми следами в устройствах, реализующих концепцию интернета вещей, должны производиться с обязательным участием специалиста во избежание потери информации.

SOME ASPECTS OF USING THE CONCEPT OF «THE INTERNET OF THINGS» IN CRIME COUNTERACTION

Aleksandr B. Smuskin[1, 2]
[1] Saratov State Law Academy, Saratov, the Russian Federation
[2] Povolzhie Law Institute (branch) of All-Russian State University of Justice (RLA of Russian Ministry of Justice), Saratov, the Russian Federation

Article info

Received
2019 August 22

Accepted
2020 June 25

Available online
2020 June 30

Abstract. The author states that the era of the Internet of Things has come. It is noted that Russian law publications do not pay sufficient attention to the practical issues of law enforcement that arise from the implementation of the Internet of Things, specifically, criminalistic research and the use of smart things by law enforcement bodies. This study a first attempt at a general criminalistic analysis of implementing the concept of the Internet of Things in Russian research publications. While analyzing the practical implementation of this concept, the author concludes that it is necessary not just to single out a smart house, a smart car or smart things as different categories, but to unite them into a system of smart environment. It is noted that the elements of the public sphere of application for the Internet of Things deserve

ISSN 2500-4255

Keywords
The Internet of things; smart house; smart car; smartwatch; forensic research; electronic evidence; electronic digital traces

separate studies, while this article will only focus on everyday application. Modern obstacles to a large-scale implementation of the Internet of Things are identified. The criminalistic research of the Internet of Things and smart environment makes it possible to identify key systems that modern appliances form in this sphere, requirements to them, subsystems of a smart house, functions of smart cars and gadgets. It is stated that the criminalistic research of the subsystems of smart environment is possible with the help of scientific criminalistic findings in the sphere of electronic digital traces and electronic evidence. Key points of finding these traces are identified. The author methodically analyzes the kinds of criminalistically relevant information that could be obtained through the examination of sensors and the memory of smart things, a smart car and a smart house. The author also determines the functions whose analysis is vital for collecting evidentiary and orientation information. It is stated that all information from sensors and information devices is, in the end, accumulated in the management center, as well as in cloud and network services' servers that work with the Internet of Things. It is stressed that all interactions with electronic digital traces in the devices that implement the concept of the Internet of Things should happen with the participation of a specialist to avoid a loss of data.

Многие технологии, ранее считавшиеся только элементом фантастических книг и фильмов, сегодня получают воплощение в реальности. Конечно, до описанного футурологами мира интернета всего еще не близко, но концепция интернета вещей все более широко воплощается в жизнь. Термин «интернет вещей» был предложен Кэвином Эштоном в 1999 г. В 2008–2009 гг. произошел переход от интернета людей к интернету вещей: количество вещей, подключенных к сети Интернет, превзошло количество людей [1]. В 2020 г. рынок интернета вещей (Internet of Things), по прогнозам, превысит 1 трлн дол. [2]. Бурное развитие цифровых технологий и отставание правоохранительной сферы отмечают многие зарубежные авторы [3]. Указанные обстоятельства предопределяют необходимость изучения криминалистических аспектов использования интернета вещей. И если европейские исследователи уже признали важность разработок криминалистического обеспечения мира интернета вещей [4], то отечественные авторы пока не уделяют данному вопросу внимания, хотя и рассматривают отдельные проблемы правосубъектности техники, обладающей искусственным интеллектом [5].

Для целей данного исследования мы подразделяем применение интернета вещей на промышленное и бытовое. Криминалистические аспекты промышленного применения интернета вещей (например, при расследовании промышленного шпионажа, нарушений правил техники безопасности и правил охраны труда, совершения экологических преступлений и возможного причинения вреда жизни, здоровью и собственности иных лиц в случае взлома программ управляющего центра устройств) заслуживают отдельного исследования.

Бытовое применение интернета вещей, по нашему представлению, складывается из пользования системами «умный дом (квартира)», «умный автомобиль» [6] и носимыми гаджетами, увязанными в единую локальную сеть LAN с выходом через хаб или иное устройство в глобальную сеть Интернет. Здесь уже можно говорить об умной среде обитания. Умная среда обитания, кроме указанных выше элементов, должна включать элементы, зависящие от местных властей, например умный город (компьютеризация управления дорожным хозяйством, оповещения об экстренных ситуациях и принятия мер по их устранению, ЖКХ, перенаправления транспортных потоков и т.д.); от работодателя — умное рабочее место (компьютеризация рабочих процессов, связи и т.д.).

В настоящий момент полномасштабному применению интернета вещей, и системы «умная среда обитания» в частности, мешают только несколько преодолимых факторов:

1. Отсутствие единого протокола связи и, как следствие, невозможность реализации принципа Plug and Play (воткнул и играй, т.е. отсутствие необходимости в дополнительных установках, настройках и т.д.). Фактически для реализации идеи умного дома сама система и вся носимая техника должны быть только одной фирмы и только основного модельного ряда либо управляющий центр должен содержать данные сотен фирм о тысячах номенклатурных наименований десятков тысяч моделей.

2. Отсутствие обязательных радиометок (RFID) на предметах, упаковках продуктов питания и прочих товарах, позволяющих автома-

тически формировать список необходимых заказов и покупок и отслеживать их состояние. Подобные сенсоры, радиометки и датчики могут также использоваться для защиты от контрафактной продукции [7].

3. Высокая цена. Комплекты с максимальным набором функций только умного дома предлагаются от 800 тыс. р.[1] Реализация же всех элементов системы умной среды обитания в наших условиях может достигать десятков миллионов рублей.

4. Отсутствие гарантированной защиты от перехвата управления данными системами с преступными целями, что несет повышенную общественную опасность [8].

5. Отсутствие в системе контроля и управления доступом к устройству обоснованного баланса между правом пользователя на конфиденциальность и необходимостью внесения в устройство данных для идентификации лица. Важность баланса между идентифицируемостью и конфиденциальностью в системах интернета вещей подчеркивают многие зарубежные авторы [9–12].

В данной статье мы рассматриваем не готовые комплексы умного дома («программно-аппаратного комплекса, позволяющего автоматизировать и упростить управление различными системами, а также другим оборудованием дома или квартиры» [13]), предлагаемые отдельными фирмами (Яндекс, Ростелеком и др.), а общую (идеальную) реализацию концепции объединенной сети из уже имеющихся на рынке устройств или опытных разработок, которые уже обнародовались различными исследователями.

Система «умный дом» складывается из центра управления (сервера, хаба), датчиков сбора информации, видеокамер, маршрутизатора для выхода в Сеть и умной техники. В самом общем виде в системах «умный дом» можно выделить несколько подсистем: контроля и управления доступом, охранной и пожарной безопасности, управления климатом (отопление, вентиляция и т.д.), обеспечения комфорта (освещение, кондиционирование, увлажнение воздуха и т.д.), мультирум (распределение видео- и аудиопотоков), контроля энергопотребления[2].

Умный автомобиль, включенный в единую сеть с домом (квартирой), пока находится на уровне опытных образцов. Однако в автомобильных журналах и на соответствующих сайтах уже рассматриваются основные элементы такой системы: «Взаимодействие между автомобилем и «умным домом» начинается еще до поездки: как только человек садится в машину, дисплей отображает общую информацию о жилище. Не осталось ли открытым окно? Закрыта ли дверь? Достаточно одного жеста или нажатия пальцем, и система автоматически закроет дверь и проконтролирует обстановку в доме»[3]. Он должен оценивать загруженность дорог с помощью данных ГЛОНАСС- или GPS-систем и сети Интернет и прокладывать наиболее удобный и быстрый маршрут, оценивать состояние дороги, ее рельеф и препятствия, иметь функцию не только автопарковки, но и автопилотирования, иметь систему опознавания «свой-чужой» для определения хозяина за рулем и проезда в гараж дома или на подземный паркинг многоквартирного дома, систему отслеживания на карте для поиска в случае угона и иных ситуаций и т.д. Концепты, объединяющие некоторые или большинство из указанных функций, уже представлялись на мировых автосалонах. Умный автомобиль должен получить функцию принудительной остановки полицией (с автопарковкой) или пропуска автомобилей экстренных служб и ограничения проезда через определенную точку маршрута (например, в случае необходимости ограничения передвижения по определенной улице из-за крупного ДТП, пожара и т.д.).

Носимые умные вещи представлены широким спектром умных часов и иных гаджетов. Однако, по оценке исследователей, производители склоняются к одной из крайностей: к реализации в умных часах большинства функций фитнес-браслета (контроль здоровья и основных физических показателей владельца) или многих функций смартфона (новости, прогноз погоды, оплата касанием терминала, получение некоторых уведомлений и т.д.), но вот удачного совмещения этих крайностей пока не получается.

Элементы концепции интернета вещей могут как использоваться при совершении преступления — при взломе различных систем (взлом

[1] Умный дом: разумные варианты. URL: https://www.inspectorgadgets.ru/post/smart-home-explained.

[2] Что такое «Умный дом». URL: http://www.domelectro.ru/%D1%87%D1%82%D0%BE%D1%82%D0%B0%D0%BA%D0%BE%D0%B5%D1%83%D0%BC%D0%BD%D1%8B%D0%B9%D0%B4%D0%BE%D0%BC ; Технология «умный дом»: что это? URL: https://www.inspectorgadgets.ru/post/smart-home-explained.

[3] Какой он, умный автомобиль? URL: https://www.nalin.ru/kakoj-on-umnyj-avtomobil-5679.

системы контроля и управления доступом — нарушение неприкосновенности жилища, кража; взлом системы видеонаблюдения — нарушение неприкосновенности частной жизни; взлом банковских приложений или приложений для оплаты — кража и т.д.), так и нести на себе прямые или косвенные признаки совершения преступлений их владельцами. Нам представляется, что взлом систем умной среды обитания заслуживает отдельных научных исследований, поскольку подобный ботнет [14] создает широкий спектр угроз.

Возможность криминалистического применения концепции интернета вещей связана с выделяемой многими учеными (и нами в том числе) группой следов электронного цифрового характера [15; 16; 17, с. 47; 18; 19], а также разработками в области электронных доказательств [20–22; 23, с. 114].

С учетом наличия ряда электронных устройств, объединенных в единую сеть, представляется, что эти следы необходимо искать как на изолированных устройствах (умные часы, автомобили, иные устройства), так и в объекте, аккумулирующем информацию от всех устройств и датчиков. В рамках умной среды обитания (без учета элементов умного города и умного рабочего места) основная информация аккумулируется в центре управления.

Итак, какая же имеющая криминалистическое значение информация может быть получена из этих устройств?

Носимые гаджеты, фиксирующие физиологическое состояние пользователя, могут предоставить в распоряжение следователя большой объем косвенной информации. Как отмечают В.А. Мещеряков и А.Н. Яковлев, «проанализировав содержимое таких часов или пульсометра, мы сможем понять, где находился в конкретный момент времени владелец данного устройства, что он делал (находился в покое или подвергался физическим или эмоциональным нагрузкам), каково было его самочувствие (частота сердечных сокращений и кровяное давление). Если сопоставить эти данные с другими имеющимися в распоряжении следователя сведениями (например, в это же время в одной и той же ограниченной территориально области зарегистрированы телефоны подозреваемого и потерпевшего), то можно установить, что два субъекта встретились, скорее всего, разговаривали (датчики местоположения и скорости покажут, что они вместе стояли или, наоборот, неспешно прогуливались или ехали в автомобиле), и разговор для собеседников был «волнительный» (датчики пульса и кровяного давления зарегистрировали соответствующие отклонения от нормы)» [24, с. 290]. Кроме того, показания этих датчиков о повышении ритма сердечных сокращений, изменении ритма дыхания, повышении давления, потоотделения и т.д. могут свидетельствовать о том, что человек в уголовно-релевантное время испытывал сильные непозитивные эмоции (страх, ярость и т.д.), т.е. мог быть свидетелем преступления или сам его совершить. Показатели умных часов или фитнес-браслета могут говорить о том, что лицо прошло большую дистанцию или, наоборот, находилось в состоянии покоя и отсутствия заметных физических нагрузок, что может не соответствовать ранее данным показаниям. Также физиологические показатели могут свидетельствовать о сильной усталости лица, состоянии алкогольного или наркотического опьянения, нахождении под влиянием седативных препаратов и т.д., что будет указывать на причины дорожно-транспортного происшествия или производственного травматизма.

Из иных функций смарт-часов криминалистическое значение могут иметь бесконтактный завод автомобиля, электронный секретарь с извещением в установленное время о запланированном мероприятии, бесконтактные платежи (например, Google Pay) и мобильные платежи, уведомление о звонках и сообщениях, фотосъемка, GPS-модуль.

Выявление электронных цифровых следов завода автомобиля в определенное время может опровергать ранее данные показания об угоне автомобиля или его нерабочем состоянии, о нахождении владельца в ином месте или его бессознательном состоянии и т.д.

Платежная информация умных часов может подтвердить совершение платежей или получение некоторых сумм от лиц, связанных с совершением преступления.

Уведомления смарт-часов могут подтвердить получение некой информации владельцем в уголовно-релевантное время.

Электронный секретарь умных часов может содержать запись о встрече с человеком, с которым владелец смарт-часов якобы не знаком, или о необходимости посещения какого-либо места или иные записи для напоминания.

GPS-модуль умных часов поможет отследить перемещения владельца в течение дня,

основные поисковые географические запросы, проложенные маршруты с реперными точками и т.д. Следовательно, при анализе памяти смарт-часов могут быть получены фотоснимки, сделанные подозреваемым и подтверждающие нахождение его в определенном месте.

Аналогично смартфонам умные часы могут хранить аудиозаписи диктофона или телефонных переговоров. Кроме того, смарт-часы, покупаемые для контроля и обеспечения безопасности детей, могут иметь функции контроля окружающей ребенка звуковой среды, а также отображения местонахождения на карте.

Компьютеризированные системы современного автомобиля даже сейчас могут предоставить в распоряжение следователя большой объем информации. На это обращали внимание как отечественные [25], так и зарубежные ученые [26; 27]. Так, уже сейчас С.М. Колотушкин предлагает введение системы объективного контроля [28], т.е. фактически автомобильного «черного ящика». В случае же полной реализации концепта умного автомобиля с передачей автомобильной информации в единый управляющий центр умной среды обитания можно будет в ходе следственного осмотра с помощью специалиста и ряда аппаратно-технических средств получить информацию о маршруте движения, точках и времени остановок, совпадении нахождения автомобилей интересующих следствие лиц в одном месте в одно время, механизме ДТП (по показаниям датчиков автомобиля можно восстановить трехмерную картину ДТП), нарушении правил дорожного движения, действиях водителей, физиологическом состоянии водителей с помощью датчиков выдыхаемого алкоголя и датчиков усталости[4], режиме движения и парковки (автоматический или ручной), а также видеозаписи видеорегистраторов, данные о попытках взлома и срабатывании сигнализации, аутентификации пользователей и т.д.

Сочетание датчиков и средств видеофиксации систем умного дома позволит полностью восстановить все действия владельцев: идентификацию их системами контроля и управления доступом (здесь следует учитывать перспективы развития биометрических технологий, важность которых подчеркивали многие авторы, особенно за рубежом [29], еще десять лет назад); проход в дом (квартиру) пользователя системы в одиночку, с членами семьи или ранее незарегистрированными в системе пользователями (это же можно установить по автоматическому изменению климатических настроек в помещении, объему продуктов, использованных автоматическими и полуавтоматическими средствами готовки, данным посудомоечной машины об использованной посуде и т.д.). Резкое изменение настроек прослушиваемых стилей музыки, типов фильмов, телепрограмм может свидетельствовать о появлении нового гостя у владельца умного дома.

Данные датчиков освещения могут подтвердить или опровергнуть информацию о том, работало или спало допрошенное лицо. Система мультирум и компьютерное оборудование дома могут раскрыть информацию о проведении лицом досуга (просмотр фильмов, прослушивание аудиокниг, музыки, видеоигры). Повышенная громкость фильмов, звукового сопровождения игр, музыки, запуск музыки определенных стилей и направлений (heavy metal rock, hardcore и т.д.), усиление яркости освещения могут наводить на сомнения относительно показаний о том, что лицо спало.

Компьютерные системы дома могут хранить так называемую дорожку электронных следов [21, с. 335] — совокупность следов отражения действий пользователя компьютерного устройства. С учетом развивающейся тенденции к сопряжению телевизионных устройств, компьютера и смартфона представляется, что в расширенных системах мультирум будет также информация об аудиовидеоконтактах лица и т.д.

Дистанционные датчики умного дома, направленные на контроль здоровья лица, связанные с аналогичными датчиками смарт-часов и автомобилей, могут оперативно фиксировать показатели здоровья лица и его психоэмоционального состояния. Соответственно, с помощью этих датчиков будет точно установлено время эмоционально сложного разговора или

[4] Датчики усталости уже сейчас устанавливаются в некоторые дорогие модели Volkswagen и Mercedes. Датчики усталости на автомобиле Volkswagen делают вывод об ослаблении внимания на основании характера подергивания рулем, что типично для уставших водителей. Сложные системы, как на моделях Mercedes, в первые минуты езды запоминают типичную для данного водителя манеру управления автомобилем. Они анализируют время суток и продолжительность непрерывной езды. Базовые данные дополняются информацией, поступающей от более чем 70 датчиков. Проанализировав все данные, система предупреждает символом на спидометре (чашка кофе) и звуковым сигналом (Все о вспомогательных системах автомобиля // Пособие автомобилиста. URL: https://sanekua.ru/vse-o-vspomogatelnyx-sistemax-avtomobilya).

время причинения вреда здоровью или жизни лица, будут вызваны экстренные службы.

Электронные следы в памяти управляющего центра о включении света в разных помещениях могут указывать на перемещение владельца или иного лица по дому (квартире) в то время, когда там никого не должно быть. Однако при этом необходимо принимать во внимание настраиваемую в умном доме функцию имитации световой активности[5].

При производстве расследований с использованием электронных цифровых следов в устройствах систем интернета вещей следует принимать во внимание, что даже в случае уничтожения или модификации следов в конкретном устройстве они могут сохраниться в центре управления умного дома либо в облачных сервисах, задействованных в реализации рассматриваемой концепции.

Любые действия с электронными цифровыми следами в указанных устройствах во избежание утери информации могут предприниматься следователем с обязательным участием специалиста и применением соответствующих программно-аппаратных комплексов, а также с соблюдением иных криминалистических рекомендаций по работе с электронными носителями информации и электронными цифровыми следами.

Таким образом, при оптимальном использовании правоохранительными органами данных, сохраненных в памяти умных устройств при реализации концепции интернета вещей, с учетом наработок складывающейся в настоящее время частной теории криминалистического исследования и использования электронной цифровой информации и ее носителей (электронной цифровой криминалистики)[6] следствие получает новые доказательственные возможности и эффективный инструментарий расследования преступлений.

[5] «Умный дом» — переосмысление. URL: https://m.habr.com/ru/post/444852.

[6] Подробное обоснование наименования данной частной криминалистической теории представлено нами в иных произведениях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Пилипенко Н. Интернет вещей — а что это? / Н. Пилипенко // Хабр. — 2012. — 15 авг. — URL: https://m.habr.com/ru/post/149593.

2. Койфман Я. Рынок на триллион: как защитить «умный дом» от хакеров / Я. Койфман // Forbes. — 2018. — 10 мая. — URL: https://yandex.ru/turbo/s/forbes.ru/tehnologii/360979-rynok-na-trillion-kak-zashchitit-umnyy-dom-ot-hakerov.

3. Gavin J.D. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach / J.D. Gavin, B.M. Lyria, Ch. Janet // The British Journal of Criminology. — 2017. — Vol. 57, iss. 2. — P. 259–274.

4. Tecklenborg T. Häuser mit Smart Home Technologie als Ziele von Einbrechern / T. Tecklenborg, A. Stupperich // Kriminalistik. — 2018. — № 72 (4). — S. 203–207.

5. Шестак В.А. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России / В.А. Шестак, А.Г. Волеводз. — DOI: 10.17150/2500-4255.2019.13(2).197-206 // Всероссийский криминологический журнал. — 2019. — Т. 13, № 2. — С. 197–206.

6. Татарников О. Умные автомобили / О. Татарников // КомпьютерПресс. — 2007. — № 11. — URL: https://compress.ru/article.aspx?id=18305.

7. Wang Yun. Sensor Technologies for Anti-counterfeiting / Yun Wang, Evangelyn C. Alocilja. — DOI: 10.1080/01924036.2012.726319 // International Journal of Comparative and Applied Criminal Justice. — 2012. — Vol. 36, № 4. — P. 291–304.

8. Wagen W. van der. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks / W. van der Wagen, W. Pieters. — DOI: https://doi.org/10.1093/bjc/azv009 // The British Journal of Criminology. — 2015. — Vol. 55, iss. 3. — P. 578–595.

9. Wachter S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR / S. Wachter // Computer Law & Security Review. — 2017. — Vol. 34, iss. 3. — P. 436–449.

10. Janeček V. Ownership of Personal Data in the Internet of Things / V. Janeček // Computer Law & Security Review. — 2018. — Vol. 34, iss. 5. — P. 1039–1052.

11. Weber R. Internet of Things — New Security and privacy Challenges / R. Weber // Computer Law & Security Review. — 2010. — № 26. — P. 23–30.

12. The Internet of Things (IoT) and its Impact on individual Privacy: An Australian Perspective / X. Caron, R. Bosua, S. Maynard, A. Ahmad // Computer Law & Security Review. — 2015. — Vol. 32, iss. 1. — P. 4–15.

13. Макаров Д. Что такое система умный дом и пример ее реализации / Д. Макаров // Заметки электрика. — Минск, 2020. — URL: https://www.asutpp.ru/sistema-umnyj-dom.html.

14. Wagen W. van der. The Hybrid Victim: Re-conceptualizing High-tech Cyber Victimization through Actor-network Theory / W. van der Wagen, W. Pieters // European Journal of Criminology. — 2018. — Vol. 55, № 3. — P. 578–595.

15. Мещеряков В.А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе / В.А. Мещеряков // Воронежские криминалистические чтения : сб. науч. тр. — Воронеж, 2008. — Вып. 9. — С. 221–232.

16. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09 / В.Ю. Агибалов. — Воронеж, 2010. — 24 с.

17. Першин А.Н. «Временные следы» при расследовании преступлений, совершаемых с использованием компьютерных технологий / А.Н. Першин // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2016. — № 1. — С. 46–51.

18. Шаповалова Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики) : автореф. дис. … канд. юрид. наук : 12.00.09 / Г.М. Шаповалова. — Владивосток, 2006. — 21 с.

19. Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. — 2012. — № 8. — С. 43–45.

20. Основы теории электронных доказательств / под ред. С.В. Зуева. — Москва : Юрлитинформ, 2019. — 400 с.

21. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : дис. … д-ра юрид. наук : 12.00.09 / В.Б. Вехов. — Волгоград, 2008. — 401 с.

22. Пастухов П.С. Средства проверки надежности «электронных» доказательств в ходе производства по уголовному делу / П.С. Пастухов // Пробелы в российском законодательстве. — 2015. — № 3. — С. 170–173.

23. Россинская Е.Р. Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» / Е.Р. Россинская // Деятельность правоохранительных органов в современных условиях : междунар. науч.-практ. конф., Иркутск, 23–24 мая 2017 г. В 2 т. Т. 2. — Иркутск, 2018. — С. 113–118.

24. Мещеряков В.А. «Электронная» составляющая осмотра места происшествия / В.А. Мещеряков, А.Н. Яковлев // Библиотека криминалиста. — 2015. — № 5 (22). — С. 280–291.

25. Бережной И.А. Современный автомобиль как объект цифровых исследований / И.А. Бережной // E-Forensics Russia, 2018 : междунар. конф. — URL: https://www.youtube.com/watch?v=7c2FziMVwmE.

26. Brummer P. Das Kraftfahrzeug als Beweismittel Digitale Fahrzeugdaten und ihre polizeiliche Relevanz in der analogen Welt / P. Brummer, M. Hoch // Kriminalistik. — 2017. — URL: https://www.kriminalistik.de/ausgabe/inhalt-der-ausgabe-november-2017#Artikel1.

27. Grabowski T. Vernetzte Fahrzeuge: Neue Ermittlungsansätze im Strafverfahren? / T. Grabowski. // Kriminalistik. — 2018. — URL: https://www.kriminalistik.de/ausgabe/inhalt-der-ausgabe-April-2018#Artikel2.

28. Колотушкин С.М. Обязательное использование видеорегистраторов на автотранспортных средствах как элемент в концепции безопасности дорожного движения / С.М. Колотушкин // Электронные носители информации в криминалистике : материалы круглого стола. — Москва, 2016. — С. 30–33.

29. Neyland D. Who's Who?: The Biometric Future and the Politics of Identity / D. Neyland // European Journal of Criminology. — 2009. — Vol. 6, № 2. — P. 135–155.

REFERENCES

1. Pilipenko N. The Internet of Things: what is it? *Khabr*, 2012, August 15. Available at: https://m.habr.com/ru/post/149593. (In Russian).

2. Koifman Ya. A trillion market: how to protects a «smart house» against hackers. *Forbes*, 2018, May 10. Available at: https://yandex.ru/turbo/s/forbes.ru/tehnologii/360979-rynok-na-trillion-kak-zashchitit-umnyy-dom-ot-hakerov. (In Russian).

3. Gavin J.D., Lyria B.M., Janet Ch. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*, 2017, vol. 57, iss. 2, pp. 259–274.

4. Tecklenborg T., Stupperich A. Häuser mit Smart Home Technologie als Ziele von Einbrechern. *Kriminalistik*, 2018, no. 72 (4), S. 203–207.

5. Shestak V.A., Volevodz A.G. Modern Requirements of the legal Support of artificial Intelligence: a view from Russia. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 2, pp. 197–206. DOI: 10.17150/2500-4255.2019.13(2).197-206. (In Russian).

6. Tatarnikov O. Smart cars. *Komp'yuterPress = ComputerPress*, 2007, no. 11. Available at: https://compress.ru/article.aspx?id=18305. (In Russian).

7. Wang Yun, Alocilja E.C. Sensor Technologies for Anti-counterfeiting. *International Journal of Comparative and Applied Criminal Justice*, 2012, vol. 36, no. 4, pp. 291–304. DOI: 10.1080 / 01924036.2012.726319.

8. Wagen W. van der, Pieters W. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *The British Journal of Criminology*, 2015, vol. 55, iss. 3, pp. 578–595. DOI: https://doi.org/10.1093/bjc/azv009.

9. Wachter S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR / S. Wachter // Computer Law & Security Review, 2017, vol. 34, iss. 3, pp. 436–449.

10. Janeček V. Ownership of Personal Data in the Internet of Things. *Computer Law & Security Review*, 2018, vol. 34, iss. 5, pp. 1039–1052.

11. Weber R. Internet of Things — New Security and privacy Challenges. *Computer Law & Security Review*, 2010, no. 26, pp. 23–30.

12. Caron X., Bosua R., Maynard S., Ahmad A. The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective. *Computer Law & Security Review*, 2015, vol. 32, iss. 1, pp. 4–15.

13. Makarov D. What is a smart house system and how it can be implemented. *Zametki elektrika = Electrician's Notes.* Minsk, 2020. Available at: https://www.asutpp.ru/sistema-umnyj-dom.html. (In Russian).

14. Wagen W. van der, Pieters W. The Hybrid Victim: Re-conceptualizing High-tech Cyber Victimization through Actor-network Theory. *European Journal of Criminology*, 2018, vol. 55, no. 3, pp. 578–595.

15. Meshcheryakov V.A. Digital (virtual) Traces in Criminalistics and Criminal Proceedings. *Voronezhskie kriminalisticheskie chteniya* [Voronezh Criminalistic Readings]. Voronezh, 2008, iss. 9, pp. 221–232. (In Russian).

16. Agibalov V.Yu. *Virtual'nye sledy v kriminalistike i ugolovnom protsesse. Avtoref. Kand. Diss.* [Virtual Traces in Criminalistics and Criminal Proceedings. Cand. Diss. Thesis]. Voronezh, 2010. 24 p.

17. Pershin A.N. «Time Track» in the Investigation of Crimes Committed Using Computer Technology. *Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologii: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenii =*

Crime in the Sphere of Information and Telecommunication technologies: Problems of Prevention, Detection and Investigation of Crimes, 2016, no. 1, pp. 46–51. (In Russian).

18. Shapovalova G.M. *Vozmozhnost' ispol'zovaniya informatsionnykh sledov v kriminalistike (voprosy teorii i praktiki). Avtoref. Kand. Diss.* [The possibility of using information traces in criminalistics (issues of theory and practice). Cand. Diss. Thesis]. Vladivostok, 2006. 21 p.

19. Smushkin A.B. Virtual Traces in Criminalistics. *Zakonnost' = Legality*, 2012, no. 8, pp. 43–45. (In Russian).

20. Zuev S.V. (ed.). *Osnovy teorii elektronnykh dokazatel'stv* [Fundamentals of the Theory of Electronic Evidence]. Moscow, Yurlitinform Publ., 2019. 400 p.

21. Vekhov V.B. *Kriminalisticheskoe uchenie o komp'yuternoi informatsii i sredstvakh ee obrabotki*. *Dokt. Diss*. [The Criminalistic Doctrine about Computer Information and Means of its Processing. Doct. Diss.]. Volgograd, 2008. 401 p.

22. Pastukhov P.S. Means of Verification Reliability «Electronic» Evidence in Criminal Proceedings. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian legislation*, 2015, no. 3, pp. 170–173. (In Russian).

23. Rossinskaya E.R. The concept of a private criminalistic theory «information and computer support of criminalistic work». *Deyatel'nost' pravookhranitel'nykh organov v sovremennykh usloviyakh. Materialy 23-i mezhdunarodnoi nauchno-prakticheskoi konferentsii, Irkutsk, 23–24 maya 2018 g.* [Activities of the Law Enforcement Bodies in the Current Conditions. Materials of the 23nd International Scientific and Practical Conference, Irkutsk, May 23–24, 2018]. Irkutsk, 2018, vol. 2, pp. 113–118. (In Russian).

24. Meshcheryakov V.A., Yakovlev A.N. The «Electron» Constituent of view of Place of Occurrence under Investigation. *Biblioteka kriminalista = Library of a Criminalist*, 2015, no. 15 (22), pp. 280–291. (In Russian).

25. Berezhnoi I.A. Modern automobile as an object of digital research. *E-Forensics Russia 2018. International Conference.* Available at: https://www.youtube.com/watch?v=7c2FziMVwmE. (In Russian).

26. Brummer P., Hoch M. Das Kraftfahrzeug als Beweismittel Digitale Fahrzeugdaten und ihre polizeiliche Relevanz in der analogen Welt. *Kriminalistik,* 2017. Available at: https://www.kriminalistik.de/ausgabe/inhalt-der-ausgabe-november-2017#Artikel1.

27. Grabowski T. Vernetzte Fahrzeuge: Neue Ermittlungsansätze im Strafverfahren? *Kriminalistik*, 2018. Available at: https://www.kriminalistik.de/ausgabe/inhalt-der-ausgabe-April-2018#Artikel2.

28. Kolotushkin S.M. Obligatory use of car dashboard cameras as an element of the concept of safe driving. *Elektronnye nositeli informatsii v kriminalistike*. *Materialy kruglogo stola* [Electronic media in Criminology. Materials of a Round Table]. Moscow, 2016, pp. 30–33. (In Russian).

29. Neyland D. Who's Who?: The Biometric Future and the Politics of Identity. *European Journal of Criminology*, 2009, vol. 6, no. 2, pp. 135–155.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Смушкин Александр Борисович — доцент кафедры криминалистики Саратовской государственной юридической академии, доцент кафедры уголовно-правовых дисциплин Поволжского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук, доцент, г. Саратов, Российская Федерация; e-mail: skif32@ya.ru.

INFORMATION ABOUT THE AUTHOR

Smuskin, Aleksandr B. — Ass. Professor, Chair of Criminalistics, Saratov State Law Academy, Ass. Professor, Chair of Criminal Law Disciplines, Povolzhie Law Institute (branch) of All-Russian State University of Justice (RLA of Russian Ministry of Justice), Ph.D. in Law, Ass. Professor, Saratov, the Russian Federation; e-mail: skif32@ya.ru.

ДЛЯ ЦИТИРОВАНИЯ

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

FOR CITATION

Smuskin A.B. Some aspects of using the concept of «the Internet of things» in crime counteraction. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460. (In Russian).