

УДК 343.9

Bluetooth-трекеры: обзор устройств и значимость для экспертного исследования

Караваева Анастасия Владимировна

karlova_av@bmstu.ru

SPIN-код: 8696-6670

Абрашкова Александра Владимировна

abrashkovaav@student.bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. Рассмотрены современные персональные Bluetooth-трекеры как устройства для отслеживания местоположения объектов в реальном времени. Проведен обзор развития рынка трекеров и их широкого применения, включая продукты таких компаний как Tile, Samsung и Apple. Отмечена растущая актуальность криминалистического анализа данных, получаемых с этих устройств, в связи с участившимися случаями их использования в противоправных целях, таких как stalking и незаконное слежение. Описан механизм работы краудсорсинговой сети, обеспечивающей определение геолокации трекеров через мобильные устройства-Helper. Обусловлена актуальность исследования Bluetooth-трекеров и данных из мобильных приложений в рамках судебной компьютерно-технической экспертизы.

Ключевые слова: Bluetooth-трекеры, персональные отслеживающие устройства, судебная компьютерно-техническая экспертиза, данные мобильных устройств, технология Bluetooth Low Energy

Bluetooth trackers: a review of devices and importance for expert research

Karavaeva Anastasia Vladimirovna

karlova_av@bmstu.ru

SPIN-code: 8696-6670

Abrashkova Alexandra Vladimirovna

abrashkovaav@student.bmstu.ru

BMSTU, Moscow, Russia

Abstract. The article considers modern personal Bluetooth trackers as devices for tracking the location of objects in real time. An overview of the tracker market development and their widespread use, including products from such companies as Tile, Samsung and Apple, is provided. The growing relevance of forensic analysis of data obtained from these devices is noted due to the increasing incidence of their use for illegal purposes, such as stalking and illegal surveillance. The mechanism of a crowdsourcing network that ensures the determination of tracker geolocation through mobile devices-Helper is described. The relevance of the study of Bluetooth trackers and data from mobile applications in the framework of forensic computer-technical examination is determined.

Keywords: Bluetooth-trackers, personal tracking devices, computer-forensic, mobile device data, Bluetooth Low Energy technology

Введение. Рост популярности персональных Bluetooth-трекеров вызвал потребность в разработке инструментов криминалистического и судебно-

экспертного анализа, которые помогают правоохранительным органам в установлении различных связанных с ними фактов. Так, в обзоре избранных статей по судебной экспертизе Н.В. Фетисенковой представлена аннотация статьи [1], посвященная исследованию таких устройств «Я слежу за каждым твоим шагом: судебно-экспертный анализ приложения Tile Tracker» авторов Pace L.R., Salmon L.A., Bowen C.J., Baggili I., Richard G.G., что объясняет актуальность выбранной темы.

Материалы и методы. В качестве методологической базы применены анализ и синтез положений из научных источников о видах и принципе работы Bluetooth-трекеров. Однако ускоренный темп применения персональных отслеживающих устройств не прошел бесследно, поскольку участились и сообщения об их использовании для противоправных действий [2].

Рассмотрим, что собой представляем персональное отслеживающее устройство. Трекер (трекер-метка) — это небольшого размера устройство Bluetooth Low Energy (BLE), которое при логическом подключении к мобильному устройству позволяет отслеживать его местоположение в реальном времени. Он используется для предотвращения потери личных вещей, а также для отслеживания их местоположения.

Компания Tile первой выпустила свой продукт в 2013 г., а Samsung и Apple вышли на рынок в 2021 г. с разработкой Galaxy SmartTag и AirTag. По состоянию на май 2023 г. количество зарегистрированных устройств Samsung SmartThings превысило 300 млн, в то время как примерно 55 млн AirTag и 40 млн устройств Tile было продано к 2022 г., что делает эти устройства достаточно востребованными. Рынок трекеров, оцененный в 1,78 млрд долларов в 2022 г., по прогнозам, вырастет до 16,7 млрд долларов к 2031 г. [3].

Однако вместе с этим трекеры также быстро стали использоваться и в различных преступлениях, таких как stalking, незаконное отслеживание, преступления на сексуальной почве, убийства и кражи транспортных средств. Например, в Великобритании проводились исследования преступлений, связанных со stalking с использованием искусственного интеллекта (ИИ), где ИИ обучается на данных из социальных сетей и устройств для мониторинга местоположения. В связи с имеющейся проблемой, во многих государствах уже рассматриваются законопроекты против установки или отслеживания лица с помощью трекера без его согласия. Например, в Южной Корее в 2023 г. был изменен закон о борьбе со stalking, чтобы включить в него действия, совершенные с помощью информационных и коммуникационных сетей, но он по-прежнему не охватывает трекеры. Таким образом, актуальность анализа таких устройств и данных из них не вызывает сомнений, что способствует расследованию и раскрытию преступлений [4].

Как уже было обозначено выше, сам трекер предназначен для обеспечения отслеживания местоположения объектов в реальном времени, сохраняя функциональность в течение длительного периода времени. Основная технология трекера — это BLE (Bluetooth Low Energy). Это ключевая технология,

предназначенная для применения в малопотребляющих устройствах с большими интервалами между передачей данных [5].

Таким образом, механизм получения геолокации основан на симбиозе аппаратной части самого трекера и краудсорсинговой сети. Трекер, будучи периферийным BLE-устройством, непрерывно или периодически транслирует пакеты данных. Эти пакеты содержат его уникальный идентификатор (например, хешированный MAC-адрес). В непосредственной близости (порядка 10–120 метров в зависимости от модели устройства) мобильное устройство владельца может принимать эти пакеты, устанавливать соединение и точно определять местоположение трекера относительно себя с помощью определения мощности сигнала. Ключевым аспектом является механизм, когда трекер покидает зону прямой видимости. Он продолжает транслировать свой идентификатор. Любое стороннее устройство (например, иное мобильное устройство с установленным клиентом SmartThings Find для сети Samsung или Find My для Apple), являющееся частью той самой краудсорсинговой сети и выполняющее роль Helper (не центральным устройством), детектирует этот сигнал. Helper анонимно фиксирует полученный идентификатор трекера, свои собственные точные координаты (полученные через GPS, Wi-Fi, сотовые сети) и временную метку, после чего шифрует и отправляет этот пакет данных на сервер сети. Сервер, зная, какому аккаунту принадлежит данный идентификатор трекера, ретранслирует координаты и время в приложение владельцу. Таким образом, местоположение объекта устанавливается не самим трекером (у него нет GPS-модуля), а через координаты мобильного устройства-Helper, который оказался рядом с ним [6].

Если рассматривать Bluetooth-трекеры с точки зрения объектов судебной компьютерно-технической экспертизы (СКТЭ), то данные, извлеченные из таких устройств и их экосистем, представляют собой источник криминалистически значимой информации. СКТЭ представляет собой отдельный род судебной экспертизы, относящейся к классу инженерно-технических экспертиз, целями которой являются получение доступа к информации, имеющей доказательственное значение для конкретного расследуемого дела, на представленных эксперту носителях (объектах), а также последующее изучение полученных в ходе такого доступа данных для выявления их роли в расследуемом деле. Ее объектами исследования являются компьютерная техника и (или) компьютерные (электронные) носители информации [7]. Таким образом, исследование самих Bluetooth-трекеров и данных из приложений мобильных устройств является задачей СКТЭ.

Результаты. Рассмотрим виды криминалистически значимой информации, извлекаемой из Bluetooth-трекеров и данных из приложений мобильных устройств. Во-первых, это могут быть идентификационные данные и артефакты привязки устройства. Например, уникальный идентификатор трекера (Tag ID), привязанный к нему аккаунт владельца (Apple ID, Samsung Account), дата и время активации трекера. Во-вторых, история перемещений — хронологическая последовательность координат, где был зафиксирован трекер. Каждая

точка содержит точные координаты (широта/долгота), временную метку и, что крайне важно, контекст — был ли это прямой контакт с мобильным устройством владельца или опосредованное обнаружение. Для точек, полученных через сеть, потенциально могут быть доступны метаданные устройства-Helper (например, тип устройства, уровень заряда батареи в момент обнаружения и т. д.), что может помочь в установлении круга лиц, находившихся рядом с трекером. В контексте дел о stalking или несанкционированном наблюдении история локаций трекера, сброшенного в машину или сумку жертвы, является доказательством преследования. В-третьих, это — геолокация, т. е. точка нахождения устройства. Анализ временных меток и сопоставление времени обнаружения трекера через сеть с другими данными (например, записями с камер наблюдения, показаниями свидетелей, транзакциями по банковской карте) позволяет верифицировать так называемое «алиби».

Важность всех перечисленных видов криминалистически значимой информации обусловлена тем, что часто необходимо выявить, находилось ли устройство в определенном месте, исходя из ответа на этот вопрос будет строиться доказательственная база, по совокупности всех имеющихся доказательств можно уже говорить о том, находилось ли само лицо в тот или иной момент времени в конкретном месте [8].

Заключение. Bluetooth-трекеры представляют собой значимый объект криминалистического исследования с точки зрения СКТЭ. Их широкое распространение и использование как в легальных, так и в противоправных целях требуют развития специализированных методик анализа данных, извлекаемых из самих устройств и связанных приложений.

Список источников

- [1] Фетисенкова Н.В., Василевская Д.В. Новые публикации по судебной экспертизе. *Теория и практика судебной экспертизы*, 2024, т. 19, № 4, с. 95–101.
- [2] Волкова С.В., Караваева А.В. Решение задач геопозиционирования по совокупности данных с мобильных устройств. *Научные междисциплинарные исследования. V Междунар. науч.-практ. конф.: сб. ст.* Саратов, НОО «Цифровая наука», 2020, с. 190–193.
- [3] *Market research report*. URL: <https://www.intellectualmarketinsights.com/report/airtag-market-research-report-and-current-trends/imi-005954> (дата обращения 26.08.2025).
- [4] *Samsung tracking tag application forensics in criminal investigations*. URL: <https://www.sciencedirect.com/science/article/pii/S2666281725000149#bib13> (дата обращения 26.08.2025).
- [5] *Bluetooth Low Energy: подробный гайд для начинающих*. URL: <https://habr.com/ru/articles/532298/> (дата обращения 28.08.2025).
- [6] *Privacy Analysis of Samsung's Crowd-Sourced Bluetooth Location Tracking System*. URL: <https://arxiv.org/abs/2210.14702> (дата обращения 28.08.2025).
- [7] Баюш А.А. Судебная компьютерно-техническая экспертиза в системе судебных экспертиз. *Политехнический молодежный журнал*, 2019, № 8(37), с. 10. <https://doi.org/10.18698/2541-8009-2019-8-514>
- [8] Карлова А.В. Некоторые особенности исследования графических файлов в шестнадцатеричном формате. *Политехнический молодежный журнал*, 2019, № 7(36). <https://doi.org/10.18698/2541-8009-2019-7-50>