Секция «LegalTech. Цифровая криминалистика»

Криминалистический анализ данных с IoT-устройств: новые возможности для расследования преступлений

Научный руководитель – Комаров Игорь Михайлович

Храпач Дмитрий Сергеевич
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Юридический факультет, Кафедра криминалистики, Москва, Россия
E-mail: hrapachd@gmail.com

В последние годы можно наблюдать растущие тенденции, направленные на цифровизацию абсолютно всех сфер человеческой жизни. В ежедневном быту мы используем «умные» колонки, голосовые помощники, фитнесс-браслеты, различную бытовую технику, сервисы со встроенным искусственным интеллектом. Аналогичные системы, только более масштабные и сложные также используются и в других сферах человеческой жизнедеятельности: промышленности, государственной безопасности, финансовых системах, оборонном комплексе и так далее.

Подобные устройства объединяются общим понятием – «Интернет вещей» (англ. Internet ofThings, сокращенно IoT)[3]. Иначе говоря – Интернет вещей – это система взаимосвязанных компьютерных устройств, которые имеют функции подключения к сети Интернет, а также могут собирать и передавать данные без участия человека.

По отчетам Международного союза электросвязи, глобальное число пользователей интернета растет и в некоторых странах достигает 93 процентов от всего населения[1]. Очевидно, что с увеличением числа IoT-устройств возникает проблема их уязвимости к противоправному и несанкционированному доступу со стороны преступников. Это делает их потенциальными источниками цифровых доказательств, которые могут быть использованы в процессе расследования преступлений. В связи с этим актуальным становится вопрос о разработке методов и подходов к криминалистическому анализу данных, собираемых IoT-устройствами.

Информация о местоположении (геолокация), записи разговоров, видео с камер наблюдения, данные о перемещениях и активности пользователя являются своего рода «цифровыми следами». На данный момент в криминалистике нет единого мнения о сущности данного явления. Однако, на наш взгляд, наиболее удачное определение было сформулировано Е.Р. Россинской и И.А. Рядовским, которые считают, что цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи[2].

Такие данные могут помочь установить хронологию событий, подтвердить или опровергнуть показания подозреваемого или свидетелей, а также указать на конкретный способ совершения преступления.

В правоприменительной практике уже встречались случаи успешного использования данных, которые были получены с IoT-устройств, в целях раскрытия преступлений. Так, в 2015 году данные с фитнес-трекера Fitbit использовались в суде для опровержения ложных показаний мужчины, обвиняемого в убийстве своей жены[4]. Подсудимый утверждал, что его жена была убита злоумышленником, который ворвался в их дом. По его словам, он пытался защитить жену, но нападавший связал его, после чего убил потерпевшую. Так как убитая девушка носила фитнес-трекер Fitbit, который записывал данные о ее физической активности, анализ этих данных показал, что она продолжала двигаться в течение

некоторого времени после того, как, по словам подсудимого, она уже должна была быть мертва. Это противоречило его показаниям и указывало на то, что он мог сообщить ложную информацию о времени и обстоятельствах убийства.

Еще одним примером использования IoT-устройств в качестве доказательств по уголовному делу является дело с Amazon Echo. В Арканзасе смарт-динамик Amazon Echo стал потенциальным источником доказательств в деле об убийстве. Следователи предположили, что Echo мог записать аудио, которое могло бы содержать криминалистически-значимую информацию об обстоятельствах совершенного преступления. Они запросили у Amazon данные с устройства, включая записи и информацию о подключении. Однако компания отказалась предоставить данные, ссылаясь на защиту конфиденциальности пользователей. В итоге, данные с Echo не сыграли решающей роли в деле, но этот случай привлек внимание к вопросам конфиденциальности и использования данных с IoT-устройств в судебных разбирательствах.

В процессе расследования преступления сбор данных с IoT-устройств требует использования особых методик и передовой криминалистической техники. Применение специализированного программного обеспечения, например, инструментов для анализа данных с мобильных устройств (Cellebrite, Oxygen Forensics) или ПО для работы с конкретными IoT-платформами позволит извлекать логи, метаданные, аудио- и видеозаписи, а также данные о местоположении и активности конкретного пользователя.

Исследуя полученные сведения в совокупности с результатами иных следственных действий: допросов, очных ставок, осмотров и так далее, следователь сможет с наибольшей вероятностью установить все обстоятельства, подлежащие доказыванию.

Криминалистический анализ данных с IoT-устройств открывает новые горизонты для расследования преступлений. Однако эффективное и правомерное их применение сопряжено с рядом проблем, начиная от отсутствия соответствующих методических рекомендаций и техники и заканчивая балансом между интересами правоохранительных органов и защитой личных данных пользователей. Таким образом, IoT-устройства становятся не только частью повседневной жизни, но и важным инструментом в борьбе с преступностью.

applewebdata://045BEF30-80B3-46CA-9C48-6E2019CFE97D#_ftnref1

Источники и литература

1) Глобальное число пользователей интернета растет, но неравенство сохраняется. Новости ООН [Электронный ресурс] // Режим доступа: https://news.un.org/ru/story/2024/11/1458816 (Дата обращения: 20.02.2025)

2) Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019

3) Ashton, K. (22 June 2009). «That «Internet of Things» Thing» [Электронный ресурс] // Режим доступа: http://www. rfidjournal.com/articles/view?4986 (Дата обращения: 20.02.2025)

4) Man suspected in wife's murder after her Fitbit data doesn't match his alibi. The Guardian [Электронный ресурс] // Режим доступа: https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate (Дата обращения: 20.02.2025)