

Средства сотовой связи как источник криминалистически значимой информации

Конева Анна Викторовна

Дальневосточного государственного университета путей сообщения

Магистр

Аннотация

Цель данной статьи - показать на сколько тесно внедрены информационные технологии в повседневную жизнь, путем аналитического метода сбора информации.

Ключевые слова: информация, сотовая связь, мобильные технологии, криминалистические сведения, компьютерные и телекоммуникационные технологии.

Cellular communications as a source of forensic information

Koneva Anna Viktorovna

Far Eastern Transport University

Master student

Abstract

The purpose of this article: to show how closely information technology is embedded in everyday life, through the analytical method of collecting information.

Key words: information, cellular communications, mobile technologies, forensic information, computer and telecommunication technologies.

В абонентских устройствах содержатся информация о контактах пользователя, из которой можно извлечь сведения о преступных связях, составе и роли участников, организованных групп, а также лицах, вовлеченных в противоправную деятельность.

Кроме того, указанные данные являются объектом криминалистического учета «записная книжка», представляющего собой базы абонентских номеров, ежедневников, контактов, изъятых у злоумышленников. Посредством указанного учета, правоохрнительными органами осуществляется сопоставление не только прямых связей интересующих лиц, но и наличие контактов через нескольких посредников.

Так же современные смартфоны оснащены камерой и имеют возможность хранения информации в виде фото и видео изображений, в которых могут содержаться криминалистически важные сведения. [5]

Криминалистически важные сведения могут также содержаться в пользовательских приложениях-объявлениях («Авито», «Юла», «ЕВау» и др.).

Так, если в Интернет-поисковике ввести номер определенного абонента, возможно, обнаружить сведения о размещении им объявлений в указанных приложениях за весь период его использования, а также данные о месте расположения. Соответственно, устанавливается не только нахождение интересующего лица, но и представляется предлог встречи якобы в целях приобретения товара (услуг), указанных в объявлении [3].

Кроме того, с помощью проверки определенных категорий объявлений возможен розыск лиц, о которых предварительно известен факт осуществления ими деятельности по продаже товаров или услуг, а также розыск похищенного имущества и др.

Одновременно, потенциальным источником криминалистически важной информации являются геолокационные данные. Функцией отслеживания перемещения абонентов посредством обслуживания базовых станций, а также спутникового сигнала (GPS или ГЛОНАСС) оснащены большинство современных смартфонов, что позволяет обнаружить устройство в случае его утери или хищения [9].

Кроме того, существуют такие шпионские программы компрометации как Talklog, Hellospy и др., созданные в целях перехвата передаваемой (получаемой) информации, обнаружение которых возможно только специальными версиями мобильных антивирусов, притом далеко не всегда.

Одновременно, в глобальной сети Интернет предлагаются сомнительные услуги отслеживания абонента без их согласия. Так, например, сервис Mobile Monitoring обещает определение расположения абонента, маршруты его движения, запись всех телефонных переговоров и др. Соответственно, сведения, предоставляемые легальным и шпионским контентом, а также услуги сотовых операторов о геолокации абонентов потенциально могут быть использованы в расследовании хищений средств сотовой связи, розыске преступников, а также лиц без вести пропавших.

Важное криминалистическое значение имеют также сведения, полученные из современных приложений-Messenger, которые представляют собой программы для быстрого обмена текстовыми сообщениями, фото и видео файлами и передачи визуального и звукового сигнала через веб-камеры (Viber, IMO, WhatsApp, SKYPE и др.). [9]

Кроме того, наравне с Messenger в абонентских устройствах популярно использование социальных сетей («Одноклассники», «ВКонтакте», «Инстаграм» и др.), имеющих возможность создания личной странички абонентов, на которой размещаются фотографии, аудио и видеозаписи и др.

Соответственно, это расширяет возможности извлечения криминалистически значимой информации о пользователях.

Любая информация, возникающая в ходе эксплуатации пользовательского оборудования непосредственно в нем самом и в операционно-информационных системах и центрах коммутации оператора

подвижной связи, выступает в качестве потенциальной. А характер актуальной она приобретает тогда, когда устанавливается ее прямая причинно-следственная связь с событием преступления.

Так же суды вправе давать разрешение на получение следователем информации о телефонных соединениях всех абонентов сотовой связи, которые находились в районе совершенного и предполагаемого преступления. Данное право имеет только суд, так как подобная информация считается конфиденциальной и является частью личной жизни.

Таким образом, компьютеризация и внедрение сотовой связи в жизнь человечества неизбежна. В данное время ни один человек уже не представляют свою повседневную жизнь без сотовых телефонов. Они стали, частичкой человека, храня в себе крайне важную информацию о жизнедеятельности.

Информатизация не стоит на месте, как и технический прогресс, и сейчас мобильный телефон стал абсолютно всем для человека. Он хранит крайне важную информацию, начиная от личных фотографий, приложений с реквизитами банковских счетов, контактов и заканчивая отпечатками пальцев и данных для распознавания лица владельца. Зачастую именно эта информация «дает ход» в расследовании правонарушения. Конечно же, и много погрешностей при использовании подобной информации. Именно поэтому не стоит недооценивать всю важность, которую в себе несет просто мобильный телефон или личная страничка в социальных сетях.

Защиты информационного поля так же необходима дополнительная защита и современные методы, которые должны постоянно обновляться и развиваться.

Библиографический список

1. Вайпан В. А. Базы данных об абонентах операторов связи //Право и экономика. 2006. №. 9. С. 21-24.
2. Кириченко О.В. Информация как объект гражданских правоотношений. М.: Современное право, 2014. №9. С. 26.
3. Некеров Е. Пиратство в «Интернет»-сети. В каких случаях отвечают информационные посредники. 2015. № 4.
4. Прокофьева М.В. Мобильное и «Интернет» -телевидение: правовые проблемы организации вещания. М.: Информационное право, 2009. № 4.
5. Газета Коммерсантъ URL: <https://www.kommersant.ru>.
6. Консультант+ URL: <http://www.consultant.ru>.
7. Лекции.Ком. [Электронный ресурс]. <https://lektsii.com>. (Дата обращения 02.02.2021)
8. Официальный сайт Министерства внутренних дел. URL: www.mvd.ru.
9. Студия законов URL: <https://laws.studio.ru>. (Дата обращения 01.02.2021)
10. ELibrary- научная электронная библиотека URL: <https://www.elibrary.ru/defaultx.asp>.