

Вестник Восточно-Сибирского института МВД России. 2024. № 2 (109). С. 163–176.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024. Vol.
no. 2 (109). P. 163–176.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья

УДК 343.98

DOI: 10.55001/2312-3184.2024.86.56.014

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ИЗВЛЕЧЕНИЯ ИНФОРМАЦИИ ИЗ МОБИЛЬНЫХ УСТРОЙСТВ ПРИ ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

Куликов Алексей Геннадьевич¹, Кодзов Теймураз Нашудинович²

¹ Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация

² Северо-Кавказский институт (филиал) Краснодарского университета
МВД России, г. Нальчик, Российская Федерация

¹ alex_25051970@mail.ru

² mvd.kodzov@mail.ru

Введение. Данная научная статья посвящена исследованию проблемных вопросов, связанных с использованием средств извлечения информации из памяти электронных носителей информации в ходе проведения оперативно-розыскных мероприятий. В современном информационном обществе мобильные устройства становятся неотъемлемой частью жизни людей, содержащих огромное количество персональной информации. Эта информация может быть полезной для правоохранительных органов при проведении оперативно-розыскных мероприятий и следственных действий. Статья подробно изучает различные методы и средства извлечения информации из мобильных устройств, включая программное и аппаратное обеспечение, применяемые в процессе обработки информации с целью получения доказательств. Авторы статьи анализируют существующие подходы к извлечению информации, обращаются к актуальным научным исследованиям и предлагают собственные рекомендации по использованию этих средств в рамках оперативно-розыскной деятельности. Ключевые аспекты, рассмотренные в статье, включают выбор подходящих инструментов для извлечения информации, анализ правового аспекта использования этих средств, методы обработки и защиты данных, а также соображения в области конфиденциальности.

Материалы и методы. Нормативную базу исследования составили Конституция Российской Федерации; оперативно-розыскное законодательство; иные федеральные законы; акты официального толкования норм; подзаконные нормативные акты. Кроме того, методологическую основу исследования составили всеобщий диалектический метод научного познания, общенаучные методы познания и некоторые частнонаучные методы, среди которых: анализ, сравнение, обобщение оперативно-следственной и экспертной практики, литературных и интернет-источников.

© Куликов А. Г., Кодзов Т. Н., 2024

Результаты исследования. Одним из ключевых факторов для успешной деятельности сотрудников оперативных подразделений органов внутренних дел по раскрытию преступлений, совершаемых с использованием технических средств и информационных технологий лежит в применении подобных инновационных продуктов. Это в свою очередь требует осуществления комплекса мер правового, организационного и тактического характера, направленного, в частности, на улучшение уровня материальной, технической оснащенности, формирования кадрового потенциала, способного использовать такие технические решения при решении задач оперативно-разыскной деятельности.

Выводы и заключения. В заключение авторы статьи приходят к выводу о важности эффективного использования средств извлечения оперативно значимой информации из мобильных устройств. С этой целью необходимо обеспечить подготовку специалистов, проведение научно-исследовательских работ, конференций, семинаров, круглых столов и форумов. Также важно осуществлять мониторинг зарубежного законодательства и обмениваться передовым опытом с коллегами из других стран. Эти меры помогут улучшить работу оперативных подразделений и повысить их эффективность.

Ключевые слова: оперативно-разыскная деятельность, электронные носители информации, информационно-аналитическое обеспечение, информационно-телекоммуникационные технологии, сеть Интернет, цифровые следы преступления

Для цитирования: Куликов А. Г., Кодзов Т. Н. К вопросу использования средств извлечения информации из мобильных устройств при проведении оперативно-разыскных мероприятий // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. Иркутск : Восточно-Сибирский институт МВД России. 2024. № 2 (109). С. 163–176.

DOI: 10.55001/2312-3184.2024.86.56.014

5.1.4. Criminal Law Sciences (legal sciences)

Original article

IN THE USE OF TOOLS FOR EXTRACTING INFORMATION FROM MOBILE DEVICES IN CARRYING OUT OPERATIONAL AND INVESTIGATIVE MEASURES

Alexey G. Kulikov¹, Teimuraz N. Kodzov²

¹East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation

²North Caucasus Institute (branch) of Krasnodar University Ministry of Internal Affairs of Russian Federation, Nalchik, Russian Federation

¹ alex_25051970@mail.ru

² mvd.kodzov@mail.ru

Introduction: This scientific article is devoted to the study of problematic issues related to the use of means of extracting information from the memory of electronic media in the course of operational and investigative measures. In modern information society, mobile

devices are becoming an integral part of people's lives, containing a huge amount of personal information. This information can be useful for law enforcement agencies in carrying out operational-search activities and investigative actions. The article examines in detail various methods and means of extracting information from mobile devices, including software and hardware used in the process of information processing for the purpose of obtaining evidence. The authors of the article analyze the existing approaches to information extraction, refer to current scientific research and offer their own recommendations on the use of these means in the framework of operative-search activities. Key aspects discussed in the article include the selection of appropriate tools for information extraction, analyzing the legal aspect of the use of these tools, data processing and protection techniques, and privacy considerations.

Materials and Methods: The normative basis for the study was the Constitution of the Russian Federation; operational-search legislation; other federal laws; acts of official interpretation of norms; by-laws. In addition, the methodological basis of the study was the general dialectical method of scientific knowledge, general scientific methods of knowledge and some private scientific methods, including: analysis, comparison, generalization of operational investigative and expert practice, literary and Internet sources.

The Results of the Study: One of the key factors for the successful activities of employees of operational units of internal affairs bodies in solving crimes committed using technical means and information technologies lies in the use of such innovative products. This, in turn, requires the implementation of a set of measures of a legal, organizational and tactical nature, aimed, in particular, at improving the level of material and technical equipment, and the formation of personnel potential capable of using such technical solutions in solving the problems of operational intelligence activities.

Findings and Conclusions: In conclusion, the authors of the article come to the conclusion about the importance of effectively using means of extracting operationally relevant information from mobile devices. To this end, it is necessary to ensure the training of specialists, conducting research, conferences, seminars, round tables and forums. It is also important to monitor foreign legislation and exchange best practices with colleagues from other countries. These measures will help improve the performance of operational units and increase their efficiency.

Keywords: operational search activities, electronic media, information and analytical support, information and telecommunication technologies, the Internet, digital traces of crime.

For citation: Kulikov A.G., Kodzov, T.N. K Voprosu ispol'zovaniya sredstv izvlecheniya informacii iz mobil'nyh ustrojstv pri provedenii operativno-rozysknyh meropriyatij [On the issue of using means of extracting information from mobile devices when conducting operational-search activities]. Vestnik Vostochno-Sibirskogo institute MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024, no. 2 (109), pp.163–176.

DOI: 10.55001/2312-3184.2024.86.56.014

В настоящее время сотовые телефоны стали неотъемлемыми атрибутами и практически каждый человек имеет смартфон. Активное распространение радиоподвижной связи, сети Интернет оказали существенное влияние на деятельность

правоохранительных органов [1, с. 49]. В этой связи развитие общества осуществляется в условиях цифровизации, и для сохранения конкурентоспособности на мировой арене оно должно обеспечивать основные потребности государства. Цифровые технологии стали широко использоваться делинквентами, в качестве эффективного, удобного, относительно безопасного и малозатратного для них средства и способа совершения деяний, уголовно наказуемых в большинстве стран мира [2, с. 209].

При решении задач оперативно-разыскной деятельности (далее – ОРД) оперативному сотруднику органов внутренних дел (далее – ОВД) приходится сталкиваться с необходимостью различного рода действий с цифровой информацией, так как новейшие технологии заметно расширили источники добывания оперативно значимой информацией, в том числе посредством извлечения важной электронной информации из памяти мобильных устройств [3, с. 110]. Поэтому сейчас к основным проблемам, как в организационном, тактическом, техническом, так и правовом аспектах, можно отнести деанонимизацию личности пользователя ресурсов сети Интернет, особенно в теневом его сегменте – сети DARKNET [4, с. 171].

Многочисленные исследования показывают, что определяющее влияние на эффективность деятельности органов внутренних дел оказывает знания, умения и навыки сотрудников ОВД по добыванию оперативно значимой информации, особенно содержащейся на платформе сети Интернет, а также передающейся по каналам связи [5, с. 112].

При этом на практике возникают различные проблемы, связанные не только с правовыми аспектами изъятия цифровой информации из средств связи и других носителей электронной информации, но и с недостаточным уровнем знаний практических сотрудников о специфике организации и тактике проведения оперативно-разыскных мероприятий (далее – ОРМ) и следственных действий.

Следует согласиться с мнением Е. А. Малыхиной о том, что «Борьба с преступностью играет важную роль в формировании и поддержании устойчивого правового государства. Соблюдение должного уровня правопорядка и законности – одна из приоритетных задач современного общества...» [6, с. 188].

Также следует согласиться с мнением И. Н. Железняк, который справедливо замечает, что «Законодатель же в своем нормотворчестве априори выступает в роли догоняющего, зачастую так и не сумев разобраться в процессах, выступающих катализаторами возникновения тех или иных событий, механизмах молниеносной экстраполяции существующих паттернов в обществе или, что более близко нам в исследовании, в вопросах оптимизации правил противодействия преступности...» [7, с. 67].

Верной, по нашему мнению, является позиция О. П. Грибунова о том, что «специфика рассматриваемых преступлений предопределяет некоторые особые условия, необходимые для успешного осуществления хода предварительного следствия» [8, с. 321].

Анализ практики деятельности оперативных подразделений ОВД показывает, что оперативно значимая информация, добытая указанным способом, в ряде случаев выступает единственным средством раскрытия преступления, установления истины

при расследовании уголовных дел и носит поистине неоценимое ориентирующее значение при решении различных задач ОРД.

Технические особенности сотовой связи, сети Интернет, средств обеспечения связи объективно генерируют и хранят большой массив информации, представляющей оперативно-разыскной интерес. К такой информации следует отнести:

- установочные данные пользователя;
- круг его общения;
- интересы;
- режим дня;
- медиа данные;
- маршруты передвижения и др.

В связи с этим сотовый телефон в настоящее время предстает неким объектом оперативной заинтересованности, представляя собой источник информации, который необходим при решении задач ОРД.

С точки зрения теории ОРД информация, содержащаяся в смартфонах и планшетах, принадлежащих к объектам оперативной заинтересованности, подлежит извлечению и анализу. Поэтому сотрудниками оперативных подразделений ОВД осуществляется целенаправленная деятельность по извлечению, обработке и анализу электронной информации, содержащейся на различных средствах коммуникации и связи. В данном случае для более глубокого анализа информации, содержащейся в мобильном устройстве, используются специализированные аппаратно-программные комплексы и программное обеспечение. К наиболее востребованным у сотрудников правоохранительных органов следует отнести «Мобильный криминалист», «UFED» и «XRY» [9, с. 136].

Рассмотрим более подробно основные особенности функционала и предназначение обозначенных технических решений.

«Мобильный криминалист» представляет собой программный комплекс для исследования и анализа сотовых телефонов, смартфонов и планшетов¹⁶. Принцип работы данного аппаратно-программного обеспечения основан на использовании низкоуровневых проприетарных протоколов доступа, которые позволяют извлечь большой объем данных в сравнении с логическим анализом информации. Данное программное обеспечение позволяет извлекать пользовательские данные из большинства приложений, используемых на платформах Android, iOS, Blackberry, Windows. К числу таких приложений относятся социальные сети, мессенджеры, интернет-браузеры, карты, телефонная книга, записная книга, блокнот, игры и др. Любой современный сотовый телефон содержит в себе установочные данные, контакты, сообщения, историю браузера, фотографии, видео- и аудиозаписи, сведения геолокации и т. д.

С использованием программного решения «Мобильный криминалист» оперативному сотруднику представляется возможным посредством проведения анализа данных с использованием аналитических инструментов восстановить

¹⁶ Мобильный криминалист // МКО системы : сайт.URL: <https://mko-systems.ru/mobile-expert> (дата обращения: 17.01.2024).

удаленную информацию, воссоздать хронологию событий, сформировать круг общения пользователя исследуемого устройства (рис. 1–2).

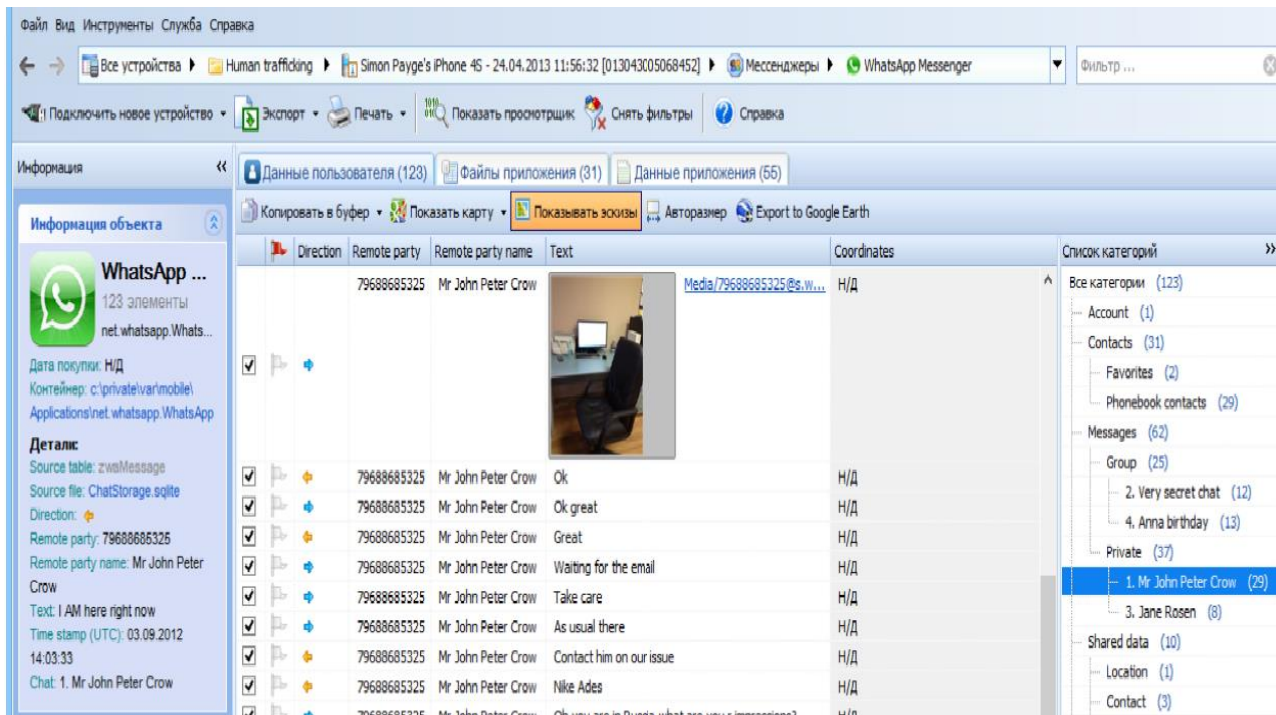


Рис. 1. Функционал программного обеспечения, позволяющий установить пароли от аккаунтов пользователей в различных социальных сетях

Приложения (8)		Общее (43)		Интернет (21)	
	Учетная запись	Пароль	Метка	Служба	
<input checked="" type="checkbox"/>	631931524	OrangeSign	ICQ	com.icq.icqfree	
<input checked="" type="checkbox"/>	alfredbobson@rocketmail.com	alfredbobson...	Yahoo! messenger	com.yahoo.messenger	
<input checked="" type="checkbox"/>	bfp51xwwrd0g2s6z2kiv	bfp51xwwrd0g...	Ebuddy	com.ebuddy.pushmessenger	
<input checked="" type="checkbox"/>	lena.soloveva.85@mail.ru	lena85@mail.ru	Mail.Ru Agent	ru.mail.agent	
<input checked="" type="checkbox"/>	lena.soloveva.85@mail.ru	lena85@mail.ru	Mail.Ru Agent	ru.mail.agent	
<input checked="" type="checkbox"/>	patrickpayge@gmail.com	patrickpayge...	Kik Messenger	com.kik.chat	
<input checked="" type="checkbox"/>	Н/Д	1234	Hide it Pro	com.smartanuj.hideitpro	
<input checked="" type="checkbox"/>	Н/Д	1234	Hide it Pro	com.smartanuj.hideitpro	

Рис. 2. Функционал средства добывания оперативно значимой информации

Интересным аспектом в практике оперативно-разыскной деятельности является функция формирования межличностных связей путем создания схем, которые позволяют выявить связи между целевым абонентом и другими лицами. Оперативный сотрудник имеет возможность использовать различные фильтры для определения

периода времени, количества связей, длительности разговоров, частоты звонков и хронологии, что позволяет выявить преступные связи интересующего лица (рис. 3).

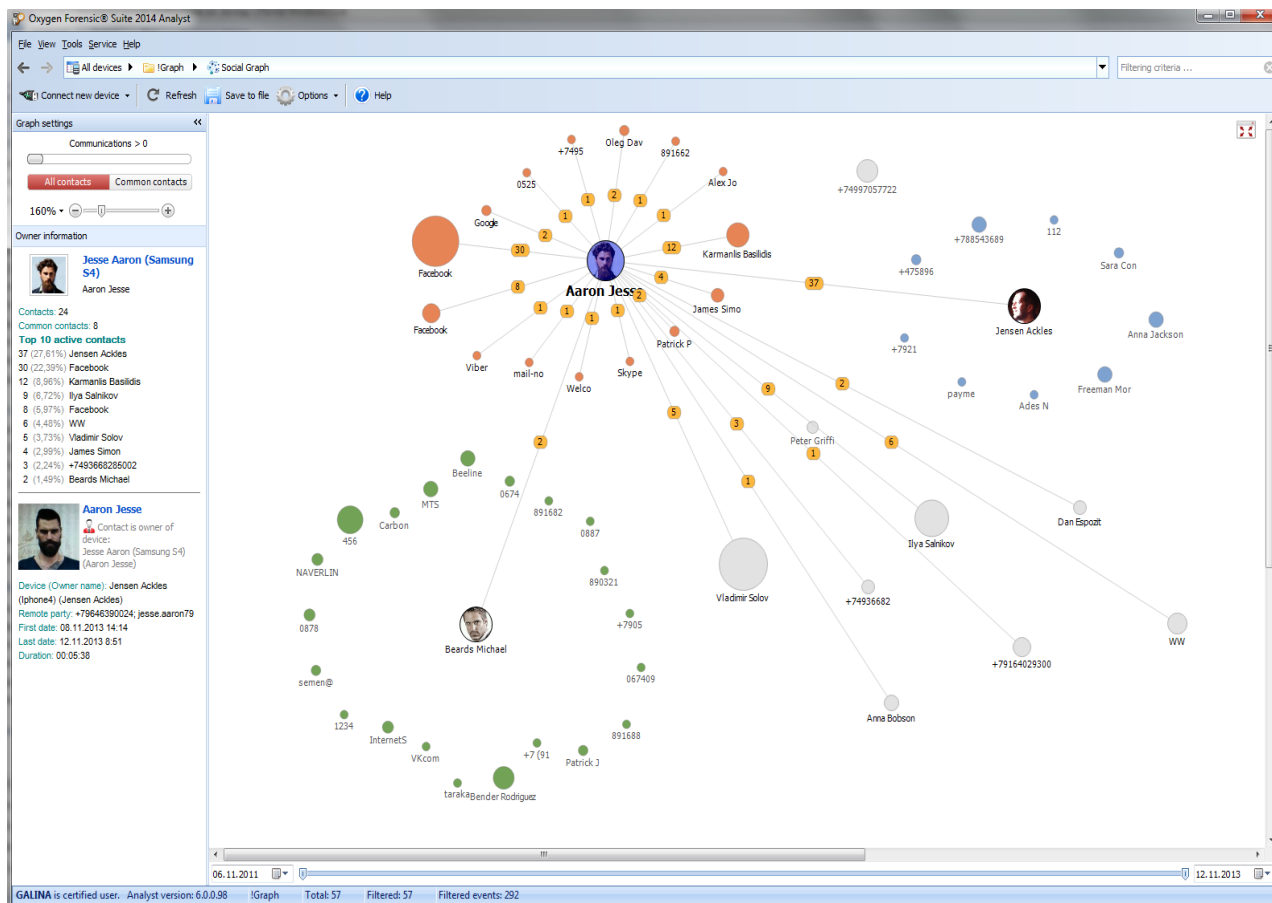


Рис.3. Фильтры, способствующие установлению периода времени, количество связей контакта, длительность разговора, частоту звонков, хронологию

Заслуживает особого внимания и функция «Веб-соединения», отображающая местоположение владельца мобильного устройства. В данном случае местоположение владельца мобильного устройства определяется по точкам WiFi-соединений, IP-подключениям и использованию баз данных геоинформационных систем. WiFi-соединения позволяют установить, где и когда лицо подключалось к сети Интернет, в том числе посредством работы с его особенностями, такими как имя (SSID), физический адрес (MAC), уровень сигнала (RSSI) и др. «Мобильный криминалист» обеспечивает извлечение данных, с помощью которых возможно определить фактическое местоположение мобильного устройства.

Использование таких данных геоинформационных систем, как «consolidated.db» и «cache_encryptedA.db» позволяют установить не только местоположение владельца мобильного устройства, но и маршруты его передвижения (рис. 4).

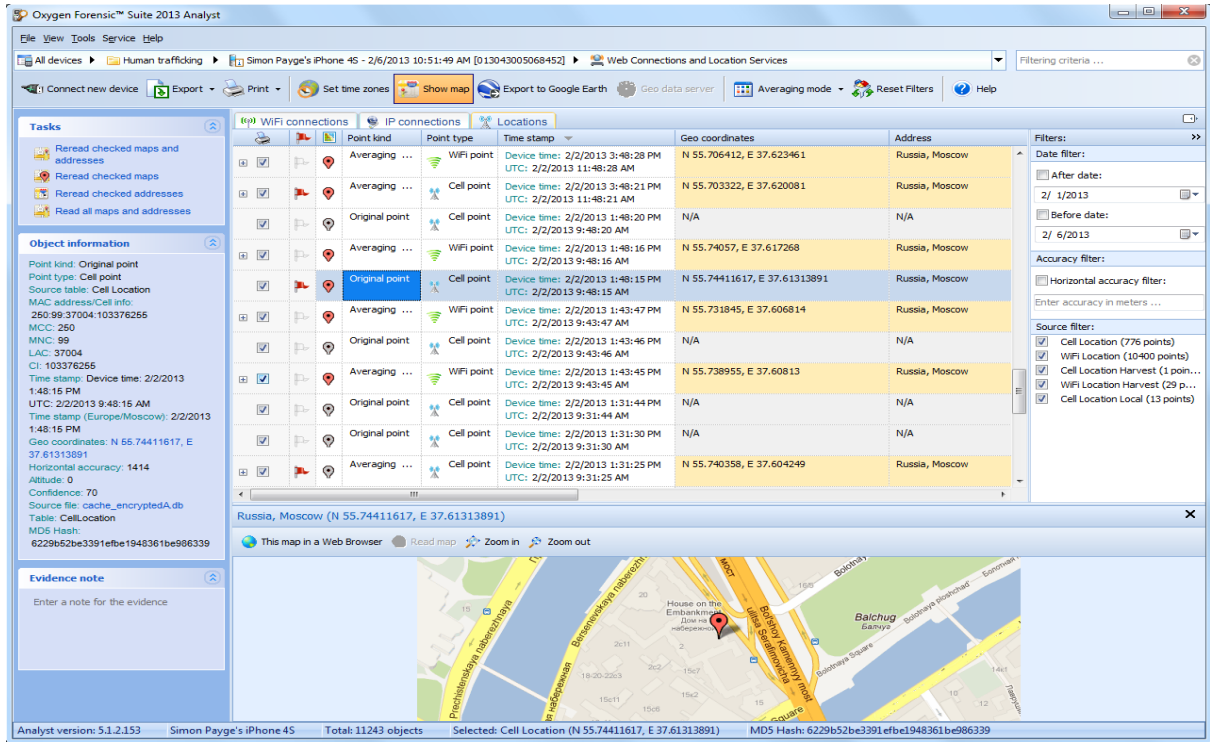


Рис. 4. Использование геоинформационной системы «consolidated.db»

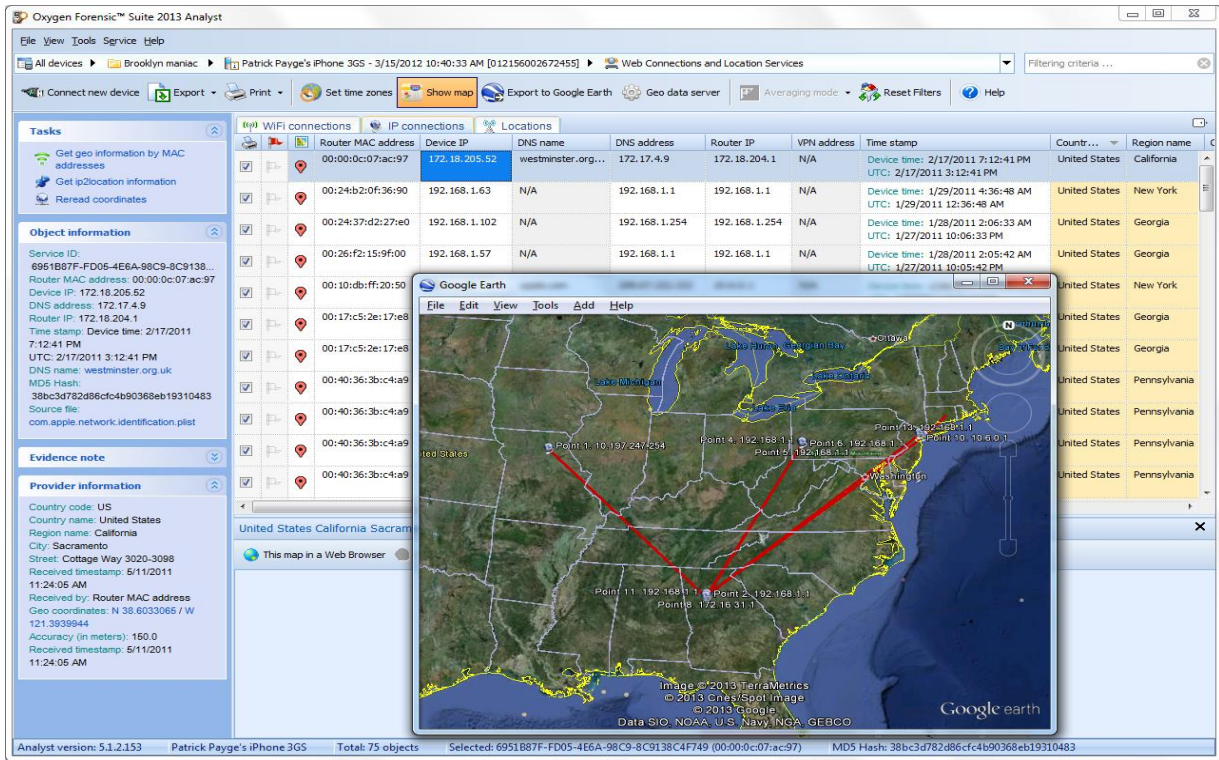


Рис. 5. Использование геоинформационной системы «cache_encryptedA.db»

Особое значение при подготовке и проведении оперативно-разыскных мероприятий имеет функция «Анализ Биллингов», которая позволяет оперативному сотруднику импортировать и анализировать биллинги, полученные от операторов сотовой связи (рис. 6).

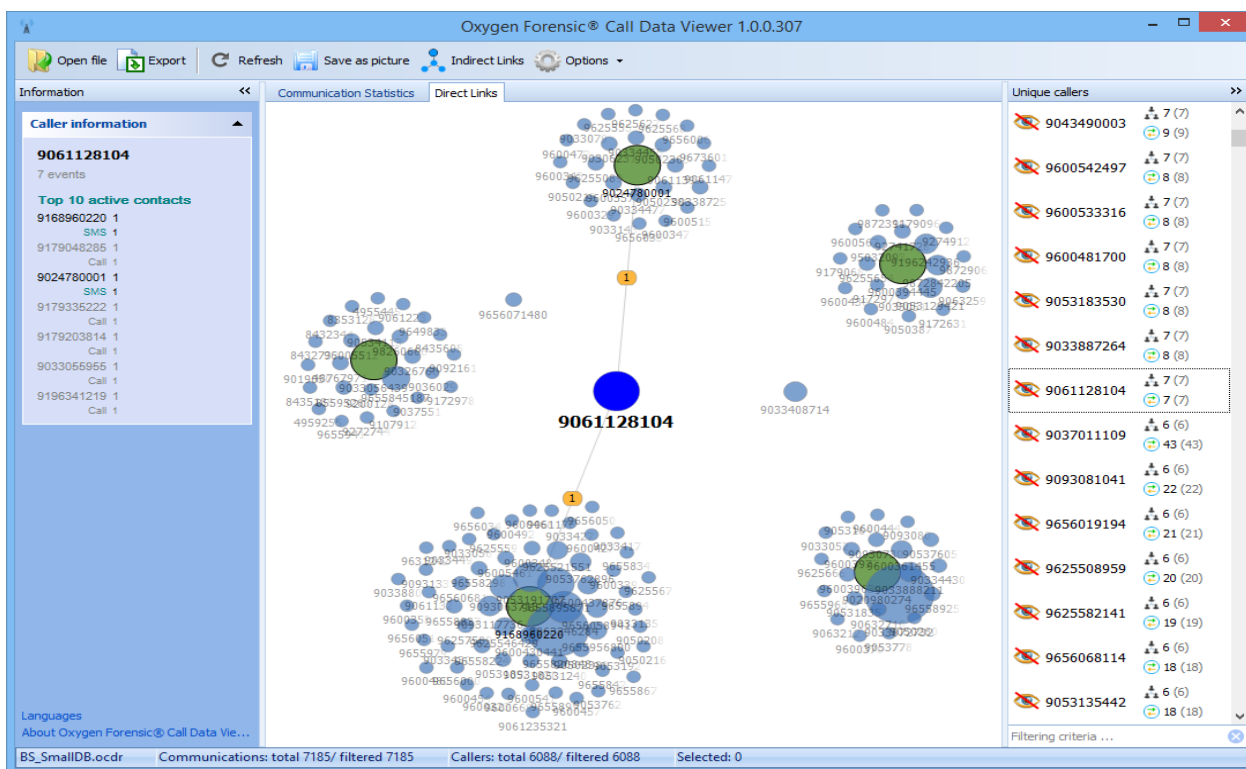


Рис. 6. Функция «Анализ биллингов»

Также в данном исследовании предлагаем рассмотреть эффективное средство технического контроля – программное обеспечение «XRY»¹⁷. Данный продукт занимает важное положение в области оперативно-разыскной деятельности, так как представляет собой комплексное аппаратно-программное решение, разработанное для операционной системы Windows, с целью безопасного извлечения оперативно значимой информации с мобильных устройств, включая смартфоны, планшеты, спутниковые навигационные системы, видеорегистраторы и т. д. Аппаратно-программный комплекс «XRY» позволяет провести полный цикл исследования, включая формирование профессионального отчета. Функционал рассматриваемого технического решения также весьма разнообразен и представлен следующими видами:

- «XRY Logical» – программное обеспечение, предназначенное для оперативного изъятия информации с мобильного устройства путем логического взаимодействия программного обеспечения с операционной системой устройства;
- «XRY Physical» – программное обеспечение, предназначенное для

¹⁷XRY // URL: <https://www.msab.com/products/xry/#physical> (дата обращения: 20.01.2024)/

физического изъятия имеющихся защищенных, скрытых, удаленных данных в памяти мобильного телефона и его последующего анализа;

- «ID SIM-Cloner» – программное обеспечение, предназначенное для клонирования «ID» SIM-карт, позволяющее сохранять целостность информации в мобильном устройстве при получении–передаче различных данных.

Аппаратно-программный комплекс «XRY» включает в себя: комплект специальных соединительных кабелей для подключения мобильных устройств; USB устройство для обеспечения совместной работы с несколькими устройствами; устройство чтения «флеш-карт»; устройство чтения SIM и micro SIM-карт; комплект SIM и micro SIM-карт для их клонирования (рис.7).



Рис. 7. Аппаратно-программный комплекс «XRY»

Рассматриваемое программное обеспечение также позволяет формировать отчеты с результатами исследований. Это устройство является компактным, удобным и информативным. Позволяет оперативно, правильно и полно оценивать полученные результаты исследования для дальнейшего использования при решении задач ОРД.

Отдельно остановимся на таком техническом решении, как «UFED»¹⁸. Данный аппаратно-программный комплекс позволяет в режиме реального времени проводить оперативные исследования мобильных устройств. Благодаря удобному и понятному

¹⁸ UFED // URL: <http://www.cellebrite.com/ru/Mobile-Lifecycle/Platforms-Products> (дата обращения: 23.05.2017).

интерфейсу и безопасному доступу оперативные сотрудники имеют возможность непосредственно извлекать пароли устройств, отключать или обходить пользовательские блокировки и декодировать данные более чем из 25 000 приложений для мобильных устройств. В процессе применения данного комплекса можно изучить практически всю деятельность пользователя.

Обобщая опыт использования таких устройств при решении задач ОРД отметим, что данные технические инновации предназначены для извлечения, восстановления, изучения информации. К такой информации следует отнести:

- пароли;
- приложения;
- данные геопозиционирования в пространстве;
- информация о местоположении абонента;
- медиа данные;
- фотографии и видеозаписи;
- содержание электронных писем;
- переписка в чатах;
- веб-история;
- детализация соединений абонента и др.

Применение подобных продуктов предусматривает обязательное соблюдение конституционных прав и свобод человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи.

Как показывает анализ практики, в деятельности правоохранительных органов отсутствует единый подход к пониманию пределов границ охраняемой законом тайны. Оперативные сотрудники ОВД, проводя анализ цифровой информации, хранящейся в памяти мобильных телефонов, не ограничиваются просмотром только содержания телефонной книги. Для получения оперативно значимой информации необходимо также просмотреть удаленные SMS-сообщения, переписку, журнал совершенных звонков и другие данные. Иногда возникают ситуации, когда оперативный сотрудник, несмотря на обязательность получения положительного судебного решения, просматривает всю информацию, содержащуюся в мобильном устройстве. Поэтому основной акцент должен быть сделан на использовании таких инноваций только при наличии судебного разрешения.

Результаты исследования практики деятельности ОВД показывают, что наиболее популярными программными инструментами среди оперативных подразделений ОВД являются «MOBILedit» и «Мобильный криминалист». Тем не менее функционал программ «UFED» и «XRY» превосходит аналогичные возможности «Мобильного криминалиста».

Одним из ключевых факторов для успешной деятельности сотрудников оперативных подразделений ОВД по раскрытию преступлений, совершаемых с использованием технических средств и информационных технологий, лежит в применении подобных инновационных продуктов. Это в свою очередь требует осуществления комплекса мер правового, организационного и тактического характера, направленного, в частности, на улучшение уровня материальной, технической

оснащенности, формирования кадрового потенциала, способного использовать такие технические решения при решении задач ОРД.

Оперативные подразделения ОВД испытывают сложности, связанные с недостаточным уровнем технического обеспечения, недостатком высококвалифицированных сотрудников и отсутствием опыта в данной сфере.

Для эффективного использования средств извлечения оперативно значимой информации из мобильных устройств необходимо обеспечить подготовку специалистов, проводить научно-исследовательские работы, конференции, семинары, круглые столы и форумы. Также важно осуществлять мониторинг зарубежного законодательства и обмениваться передовым опытом с коллегами из других стран. Эти меры помогут улучшить работу оперативных подразделений и повысить их эффективность.

СПИСОК ИСТОЧНИКОВ

1. Третьякова, Е. И. Мобильный телефон как источник криминалистически значимой информации // Вестник Уральского финансово-юридического института. – 2018. № 3(13). С. 49–51.

2. Самоделкин, А. С. Современные методы выявления и раскрытия преступлений, совершаемых с использованием цифровых технологий / А. С. Самоделкин, С. В. Тимофеев // Вестник Восточно-Сибирского института МВД России. 2022. № 2(101). С. 206–215.

3. Тимофеев, С. В. О некоторых аспектах привлечения специалиста в ходе изъятия электронных носителей информации при проведении оперативно-розыскных мероприятий / С. В. Тимофеев, В. Р. Арутюнян // Криминалистика: вчера, сегодня, завтра. 2020. № 1(13). С. 108–114.

4. Тимофеев, С. В. Деанонимизация пользователя сети Интернет как метод оперативно-розыскного противодействия наркопреступности / С. В. Тимофеев // Юристы-Правоведы. 2020. № 2(93). С. 170–174.

5. Тимофеев, С. В. К вопросу добывания оперативно значимой информации в сети интернет: проблемы и пути их решения // Криминалистика: вчера, сегодня, завтра. 2021. № 2(18). С. 111–117.

6. Малыгина, Е. А. Структура и содержание криминалистической характеристики хищений комплектующих деталей объектов железнодорожного транспорта и ее значение для частной методики расследования // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 188–200.

7. Железняк, И. Н. Дискреционность полномочий в оперативно-розыскной деятельности органов внутренних дел как маркер «ветхости» профильного закона // Общество и право. 2021. № 4 (78). С. 67–71.

8. Грибунов, О. П. Некоторые особенности производства осмотра места происшествия по делам о хищениях комплектующих деталей железнодорожного транспорта / О. П. Грибунов, Е. А. Малыгина // Современные проблемы юридической науки и правоприменительной практики: сб. науч. ст., посв. 50-летию Юридического института БФУ им. И. Канта. 2017. С. 321–327.

9. Земцова, С. И. Участие специалиста при осмотре сотового телефона по преступлениям, связанным с незаконным оборотом синтетических психоактивных веществ, совершаемым с использованием интернет-магазинов // Современное право. 2016. № 1. С. 135–141.

REFERENCES

1. Tretyakova, E. I. Mobil'nyj telefon kak istochnik kriminalisticheski znachimoj informacii [Mobile phone as a source of forensically significant information]. Vestnik Ural'skogo finansovo-yuridicheskogo institute – Vestnik of the Ural Financial and Legal Institute. 2018, no. 3(13), pp. 49-51.
2. Samodelkin, A. S. Sovremennye metody vyyavleniya i raskrytiya prestuplenij, sovershaemyh s ispol'zovaniem cifrovyyh tekhnologij [Modern methods of identifying and solving crimes committed using digital technologies]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2022, no. 2(101), pp. 206-215.
3. Timofeev, S. V. O nekotoryh aspektah privlecheniya specialista v hode iz'yatiya elektronnyh nositelej informacii pri provedenii operativno-rozysknyh meropriyatij [On some aspects of attracting a specialist during the seizure of electronic storage media during operational search activities]. Kriminalistika: vchera, segodnya, zavtra – Forensic science: yesterday, today, tomorrow. 2020, no. 1(13), pp. 108-114.
4. Timofeev, S. V. Deanonimizaciya pol'zovatelya seti internet kak metod operativno-rozysknogo protivodejstviya narkoprestupnosti [Deanonimization of an Internet user as a method of operational investigative counteraction to drug crime]. Yurist-Pravoved – Yurist-Pravoved. 2020, no. 2(93), pp. 170-174.
5. Timofeev, S. V. K voprosu dobyvaniya operativno znachimoj informacii v seti internet: problemy i puti ih resheniya [On the issue of obtaining operationally significant information on the Internet: problems and ways to solve them]. Kriminalistika: vchera, segodnya, zavtra – Forensic science: yesterday, today, tomorrow. 2021, no. 2(18), pp. 111-117.
6. Malykhina E. A. Struktura i sodержanie kriminalisticheskoy harakteristiki hishchenij komplektuyushchih detalej ob"ektov zheleznodorozhnogo transporta i ee znachenie dlya chastnoj metodiki rassledovaniya [Structure and content of forensic characteristics of thefts of components of railway transport facilities and its significance for private investigation methods]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019, no. 1 (88). pp. 188-200.
7. Zheleznyak I. N. Diskreционност' polnomochij v operativno-rozysknoj deyatel'nosti organov vnutrennih del kak marker «vethosti» profil'nogo zakona [Discretion of powers in the operational investigative activities of internal affairs bodies as a marker of the “decrepitness” of the relevant law]. Obshchestvo i pravo – Society and Law. 2021, no. 4 (78), pp. 67-71.
8. Gribunov O. P. [Some features of the inspection of the scene of an incident in cases of theft of components of railway transport] Sovremennye problemy yuridicheskoy nauki i pravoprimeritel'noj praktiki: sb. nauch. st., posv. 50-letiyu YUridicheskogo instituta BFU im. I. Kanta [Modern problems of legal science and law enforcement practice: collection. scientific art., dedicated 50th anniversary of the IKBFU Law Institute I. Kant]. 2017, pp. 321-327.
9. Zemtsova, S. I. Uchastie specialista pri osmotre sotovogo telefona po prestupleniyam, svyazannym s nezakonnym oborotom sinteticheskikh psihoaktivnyh veshchestv, sovershaemym s ispol'zovaniem internet-magazinov [Participation of a specialist during the inspection of a cell phone for crimes related to the illicit trafficking of synthetic psychoactive substances committed using online stores]. Sovremennoe pravo – Modern Law. 2016. no. 1. pp. 135-141.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Куликов Алексей Геннадьевич, старший преподаватель кафедры оперативно-разыскной деятельности. Восточно-Сибирский институт МВД России. 664074, г. Иркутск, ул. Лермонтова, 110.

ORCID: 0000-0001-6546-6563

Кодзов Теймураз Нашудинович, преподаватель кафедры огневой подготовки. Северо-Кавказский университет (филиал) Краснодарского института МВД России. 360016, Кабардино-Балкарская Республика, г Нальчик, ул. Мальбахова, д 123.

ORCID 0009-0002-4620-6947

INFORMATION ABOUT THE AUTHORS

Kulikov Alexey Gennadievich, senior lecturer of the department of operational investigative activities, East Siberian Institute of the Ministry of Internal Affairs of Russia, 664074, Russia, Irkutsk, st. Lermontova, 110.

ORCID: 0000-0001-6546-6563

Kodzov Teimuraz Nashudinovich, lecturer of the department of fire training of the North Caucasus University (branch) of the Krasnodar Institute of the Ministry of Internal Affairs of Russia, 360016, Kabardino-Balkarian Republic, Nalchik Malbakhova, st. 123.

ORCID 0009-0002-4620-6947

Статья поступила в редакцию 05.02.2024; одобрена после рецензирования 04.03.2024; принята к публикации 25.03.2024.

The article was submitted 05.02.2024; approved after reviewing 04.03.2024; accepted for publication 25.03.2024.