КРИМИНАЛИСТИКА; СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ; ОПЕРАТИВНО-РАЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

CRIMINALISTICS; FORENSIC EXPERT ACTIVITY; OPERATIONAL INVESTIGATIONS

Научная статья
УДК 343.98
DOI 10.33184/vest-law-bsu-2023.17.7

Харисова Зарина Ирековна[1, 3], Филиппов Олег Александрович[2], Нугаева Эльвира Дамировна[1, 4]
[1]Уфимский юридический институт МВД России, Уфа, Россия
[2]Уфимский университет науки и технологий, Уфа, Россия, fil.o1020@mail.ru
[3]zarinaid@mail.ru
[4]elvira.nugaeva.76@mail.ru

ИЗЪЯТИЕ КРИМИНАЛИСТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИИ С МОБИЛЬНЫХ СРЕДСТВ СВЯЗИ В РАМКАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассмотрены основные возможности использования программных средств в целях изъятия цифровых доказательств с мобильных средств связи в рамках расследования IT-преступлений, описано применение отечественного решения по проведению компьютерных экспертиз мобильных устройств.

Ключевые слова: цифровая криминалистика, форензика, цифровые доказательства, киберпреступления, расследование, экспертиза

Для цитирования: Харисова З.И. Изъятие криминалистически важной информации с мобильных средств связи в рамках расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий / З.И. Харисова, О.А. Филиппов, Э.Д. Нугаева. – DOI 10.33184/vest-law-bsu-2023.17.7 // Вестник Института права Башкирского государственного университета. – 2022. – № 4. – С. 57–64.

Original article

Kharisova Zarina Irekovna, Filippov Oleg Alexandrovich,
Nugaeva Elvira Damirovna
[1] Ufa Law Institute of the Russian Ministry of Internal Affairs, Ufa, Russia
[2] Ufa University of Science and Technologies, Ufa, Russia, fil.o1020@mail.ru
[3]zarinaid@mail.ru
[4]elvira.nugaeva.76@mail.ru

ABOUT FORENSIC INFORMATION SEARCHING FROM MOBILE COMMUNICATIONS IN THE FIELD OF CYBERCRIMES INVESTIGATION BASED ON THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Abstract. The main possibilities of software tools using to seize digital evidence from mobile communications as part of the cybercrimes investigation are shown in the paper, the use of domestic solution for conducting computer forensics of mobile devices are also described.

Keywords: digital forensics, forensics, digital evidence, cybercrime, investigation, expertise

For citation: Kharisova Z.I., Filippov O.A., Nugaeva E.D. About Forensic Information Searching from Mobile Communications in the field of Cybercrimes Investigation Based on the Use of Information and Telecommunication Technologies. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2023, no. 1, 57–64 pp. (In Russian). DOI 10.33184/vest-law-bsu-2023.17.7.

Мобильное средство связи сегодня является не только незаменимым атрибутом современного человека, средством осуществления социального взаимодействия, развлечения, получения образования, дохода, осуществления платежей [1; 2], идентификации и аутентификации в различных сервисах и информационных системах и пр., но и средством совершения преступлений. В связи с мировой тенденцией, заключающейся в возможности удаленной передачи данных, с каждым годом растет число пользователей сети Интернет, пропорционально которому увеличивается количество эксплуатируемых мобильных устройств и, соответственно, количество преступлений, совершенных с их использованием [3]. По этой причине целесообразно рассмотрение ряда узкоспециализированных, но актуальных тем, связанных с приобретением навыков эффективной фиксации, изъятия и использования цифровых доказательств с мобильных средств связи. В статье рассматрива-

ется практико-ориентированная методика, направленная на эффективное обнаружение и фиксацию цифровых артефактов в мобильных телефонах, а также изъятие криминалистически важной для расследования информации с использованием отечественного программного обеспечения «Мобильный криминалист» (далее – ПО «Мобильный криминалист») [3].

Специалистам, задействованным в расследовании киберпреступлений, необходимо владеть умениями определения взаимосвязи элементов их криминалистической характеристики, установления поводов и оснований к возбуждению уголовного дела, типичных следственных ситуаций и грамотного производства следственных действий [4], а также навыками применения в профессиональной деятельности основных алгоритмов раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Методика расследования и раскрытия преступлений, связанных с IT-составляющей, как правило, направлена на применение навыков изъятия цифровых доказательств, в частности навыков осмотра мобильного средства подозреваемого, алгоритм которого включает следующие этапы [5].

1. Перевести устройство в режим исключения приема и передачи данных для недопущения удаленного управления им.

2. Произвести полный заряд аккумулятора мобильного устройства (при наличии возможности).

3. Установить и внести в протокол учетные пользовательские данные для доступа к устройству.

4. Сбросить парольную защиту телефона.

5. Проанализировать устройство на наличие дополнительных (скрытых) пространств, с учетом установленных в них приложений.

6. Осуществить анализ установленных приложений, находящихся на момент осмотра в рабочем режиме.

7. Произвести экспорт переписки и иной значимой информации путем генерации скриншотов экрана или фотосъемки изображений на экране осматриваемого устройства.

8. Проверить историю установленных на устройстве браузеров и приложений.

9. При выявлении «криминальных» интернет-ресурсов установить и зафиксировать в протоколе пользовательские данные для доступа к ним.

10. Осуществить проверку устройства на наличие так называемых программ-шпионов. В случае обнаружения принять меры для их отключения.

11. Осмотреть содержание программ, фиксирующих заметки пользователя, календарей, ежедневников и сервиса «Документы» на наличие в них логинов и паролей, а также другой значимой информации. Уделить внима-

ние навигационным программам в целях выявления возможных мест хранения наркотиков (в том числе координат «закладок»).

12. Проверить хранилище графических изображений на наличие фотографий с информацией, способствующей изобличению задержанного в противоправной деятельности.

При проведении осмотра мобильного средства связи целесообразно действовать строго в соответствии с нормами УПК РФ, кроме того, необходимо владеть методами сбора цифровых доказательств, знать о средствах анализа машинных носителей информации (при необходимости), о существовании вспомогательных фреймворков для криминалистического анализа, программных средств на основе искусственных нейросетей [6; 7], владеть методами проведения экспертных исследований мобильных средств связи, извлечения образов мобильных операционных систем, исследования жестких дисков и энергозависимой памяти[1] [8].

Дальнейшее проведение криминалистического исследования возможно с использованием ПО «Мобильный криминалист» (см. рис. 1–3). Кроме того, возможно использование ряда популярных и свободно распространяемых специализированных утилит для проведения криминалистического анализа [8].

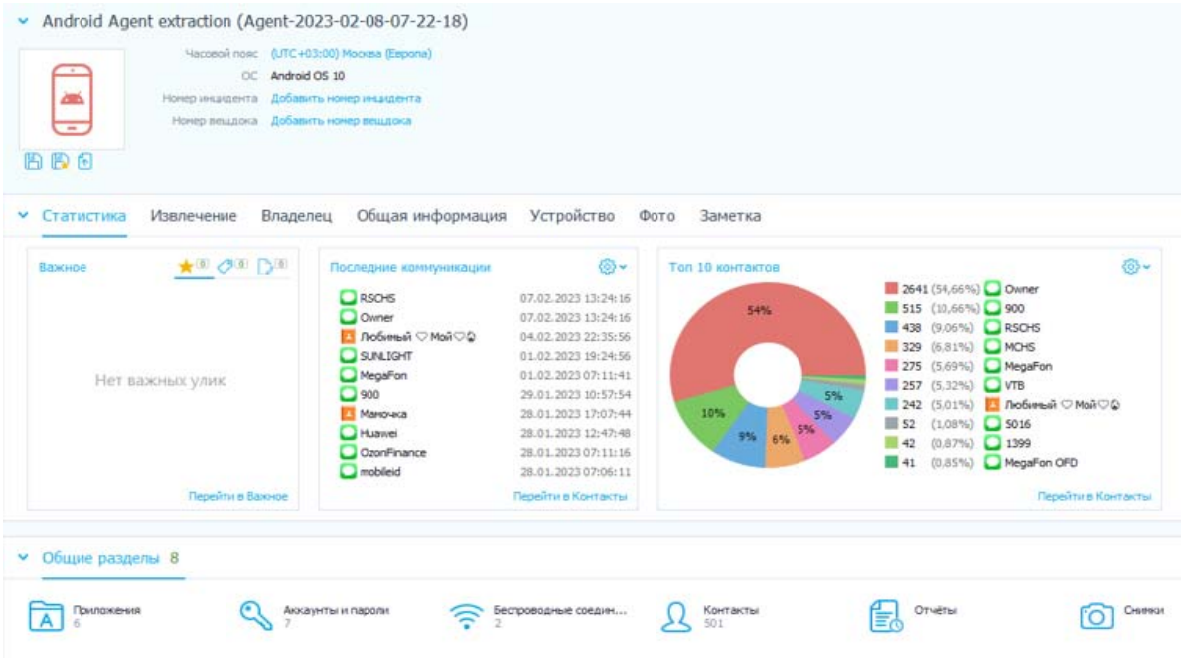

Рис. 1. Общая информация по разделам и статистические данные по исследуемому мобильному устройству в ПО «Мобильный криминалист»

[1] Харисова З.И., Нугаева Э.Д., Антонов В.В. Алгоритмический комплекс процессуальных действий при дистанционном мошенничестве «АКПД ДИСТАНТ», № 2021665929, 2021 г.; заявл. 29 июля 2021 г.; опубл. 05.10.2021.

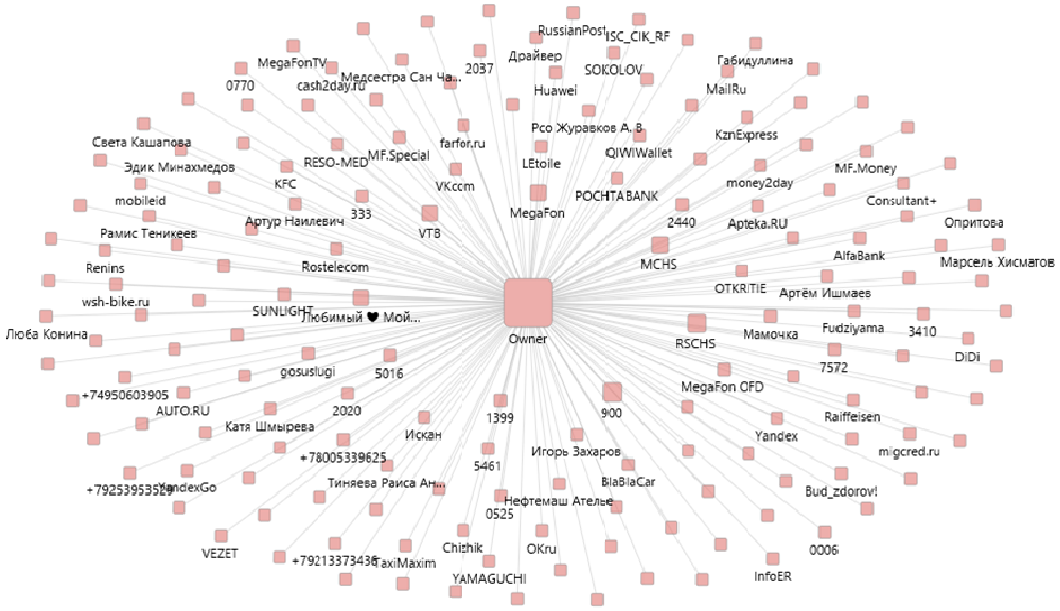

Рис. 2. Графический обзор коммуникаций между контактами, построенный в ПО «Мобильный криминалист»

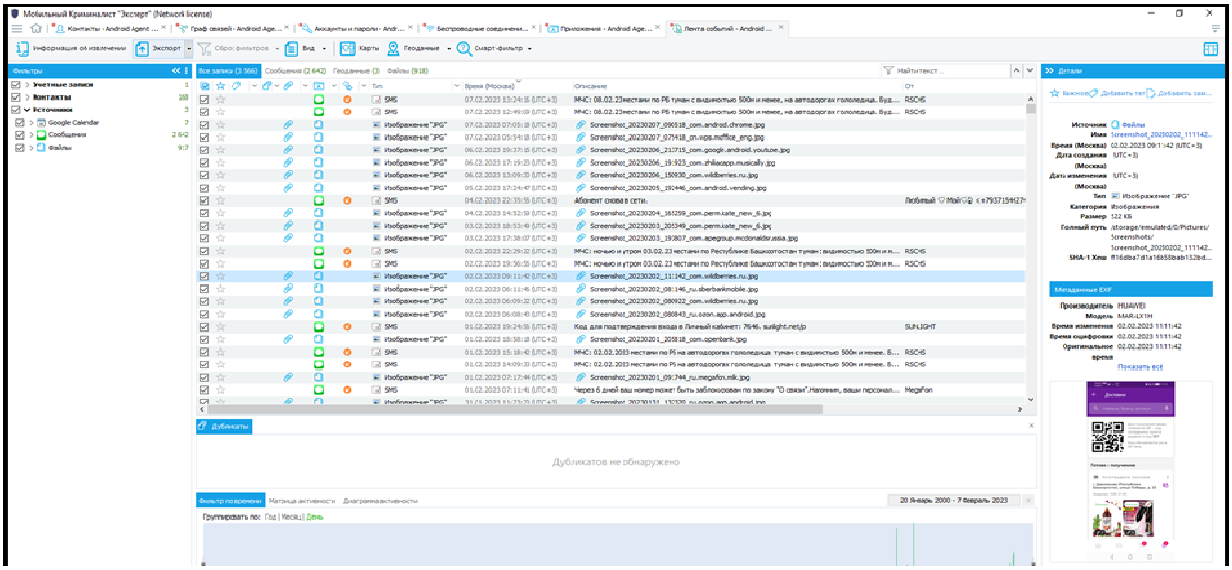

Рис. 3. Информация в разделе «Лента событий» с отражением имеющихся мультимедийных данных

Таким образом, предложенная методика изъятия криминалистически значимой информации с мобильных устройств позволит своевременно и эффективно приобщить их к уголовному делу, способствуя тем самым снижению трудозатрат при расследовании преступлений, совершенных с использованием мобильных средств связи.

Список источников

1. Харисова З.И. Обеспечение прав и свобод гражданина в области использования цифровых финансовых активов / З.И. Харисова, А.Р. Лонщакова // Евразийский юридический журнал. – 2020. – № 3 (142). – С. 167–168.

2. Ишмеева А.С. Фишинг как способ хищения денежных средств с банковских счетов / А.С. Ишмеева, И.Н. Губайдуллина // Институты и механизмы инновационного развития: мировой опыт и российская практика. – Курск, 2021. – С. 185–188.

3. Харисова З.И. О перспективах перехода органов внутренних дел на отечественное программное обеспечение в рамках импортозамещения / З.И. Харисова, А.А. Катьянова // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : сборник материалов Международной научно-практической конференции. – Уфа : БашГУ, 2019. – С. 250–256.

4. Харисова З.И. Современные угрозы информационной безопасности в условиях глобализации информационного пространства / З.И. Харисова, Р.Р. Файзулова, Д.С. Дюсьмекеева // Актуальные проблемы кибербезопасности в сети Интернет : сборник научных трудов Всероссийской конференции. – Москва, 2020. – С. 163–165.

5. Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений. – Москва : ЭКЦ МВД России, СД МВД России : ГУНК МВД России, 2020 – 18 с.

6. Антонов В.В. Системная модель интеллектуальной предметно-ориентированной профайлинг-системы / В.В. Антонов, З.И. Харисова, З.Р. Мансурова, Л.Е. Родионова, Н.Р. Калимуллин, Г.Г. Куликов // Онтология проектирования. – 2020. – Т. 10, № 3 (37). – С. 338–350.

7. Харисова З.И. Система для экспрессного определения гранулометрического состава суспензий на основе видеотехнических средств и искусственной нейросети, дообучаемой в процессе работы / З.И. Харисова, В.С. Фетисов // Приборы и системы. Управление, контроль, диагностика. – 2017. – № 2. – С. 57–64.

8. Нугаева Э.Д. Роль цифровых технологий в оптимизации криминалистической деятельности / Э.Д. Нугаева, В.Н. Чаплыгина // Актуальные проблемы уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности : сборник статей. – Орел, 2022. – С. 60–63.

References

1. Kharisova Z.I., Lonschakova A.R. Features of Information Security of the State and Society from Modern Cyber Threats. *Evrazijskij yuridicheskij zhurnal = Eurasian Law Journal,* 2020, no. 3 (142), pp. 167–168. (In Russian).

2. Ishmeeva A.S., Gubaidullina I.N. Phishing as a Way to Steal Money from Bank Accounts. *Institutions and Mechanisms of Innovative Development: World Experience and Russian Practice.* Kursk, 2021, pp. 185–188. (In Russian).

3. Kharisova Z.I., Katyanova A.A. On the Prospects of Transition of Internal Affairs Bodies to Domestic Software within the Framework of Import Substitution. *The United Nations and Global Problems of Mankind in the XXI Century. Collection of Materials of the International Scientific and Practical Conference.* Bashkir State University Publ., 2019, pp. 250–256. (In Russian).

4. Kharisova Z.I., Faizulova R.R., Dyusmekeeva D.S. Modern Threats to Information Security in the Context of Globalization of the Information Space. *Actual Problems of Cybersecurity on the Internet. Collection of Scientific Papers of the All-Russian Conference.* Moscow, 2020, pp. 163–165. (In Russian).

5. Recommendations on Cooperation between Preliminary Investigation Agencies, Operational and Forensic Units. Moscow, CEC of the Ministry of Internal Affairs of Russia, ID of the Ministry of Internal Affairs of Russia: Main Directorate for Drugs Control of the Ministry of Internal Affairs of Russia Publ., 2020, 18 p.

6. Antonov V.V., Kharisova Z.I., Mansurova Z.R., Rodionova L.E., Kalimullin N.R., Kulikov G.G. System Model of an Intelligent Domain-Oriented Profiling System. *Ontologiya proektirovaniya = Ontology of Designing,* 2020, vol. 10, no. 3 (37), pp. 338–350. (In Russian).

7. Kharisova Z.I., Fetisov V.S. System for Express Determination of Granulometric Composition of Suspensions Based on Video Equipment and an Artificial Neural Network Retrained in the Process. *Pribory i sistemy. Upravlenie, kontrol', diagnostika = Instruments and Systems. Monitoring, Control, Diagnostics,* 2017, no. 2, pp. 57–64. (In Russian).

8. Nugaeva E.D., Chaplygina V.N. The Role of Digital Technologies in the Optimization of Criminalistic Activity. *Actual Problems of Criminal Procedure Law, Criminalistics and Operational-Search Activity. Collection of Papers.* Orel, 2022, pp. 60–63. (In Russian).

Информация об авторах

Харисова Зарина Ирековна *–*
кандидат технических наук,
доцент кафедры криминалистики;

Information about the Authors

Kharisova Zarina Irekovna *–*
Candidate of Technical Sciences,
Assistant Professor of the Chair of Criminalistics;

Филиппов Олег Александрович *– кандидат юридических наук, доцент кафедры международного права и международных отношений Института права;*

Нугаева Эльвира Дамировна *– кандидат юридических наук, заведующая кафедрой криминалистики*

Filippov Oleg Alexandrovich *– Candidate of Sciences (Law), Assistant Professor of the Chair of International Law and International Relations, Institute of Law;*

Nugaeva Elvira Damirovna *– Candidate of Sciences (Law), Head of the Chair of Criminalistics*

Статья поступила в редакцию 14.02.2023; одобрена после рецензирования 14.03.2023; принята к публикации 15.03.2023.
The article was submitted 14.02.2023; approved after reviewing 14.03.2023; accepted for publication 15.03.2023.