Научная статья
УДК: 343.985.2

ТАКТИЧЕСКИЕ УСЛОВИЯ ОБЕСПЕЧЕНИЯ СОХРАННОСТИ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ГОЛОСОВОЙ ИНФОРМАЦИИ ПРИ ОСМОТРЕ МЕСТА ПРОИСШЕСТВИЯ, ПРЕДМЕТОВ, ОБЫСКЕ

Степан Евгеньевич Гольцов
Барнаульский юридический институт МВД России, г. Барнаул, Российская Федерация, S.E.Goltsov@yandex.ru

Аннотация. В настоящее время в правовой науке не были отражены тактические условия собирания криминалистически значимой голосовой информации, содержащейся на электронных носителях и в пользовательском оборудовании, в частности для обеспечения ее сохранности на подготовительном этапе осмотра места происшествия, предметов, обыска. В статье раскрываются вышеназванные условия.

Ключевые слова: голосовая информация, электронные носители, пользовательское оборудование, осмотр места происшествия, осмотр, обыск

Для цитирования: Гольцов, С. Е. Тактические условия обеспечения сохранности криминалистически значимой голосовой информации при осмотре места происшествия, предметов, обыска // Криминалистика: вчера, сегодня, завтра. 2025. Т. 36. № 4. С. 46–52.

TACTICAL CONDITIONS FOR ENSURING THE SAFETY OF CRIMINALLY SIGNIFICANT VOICE INFORMATION DURING THE INSPECTION OF THE SCENE, OBJECTS, SEARCH

Stepan E. Goltsov
Barnaul Law Institute of the MIA of Russia, Barnaul, Russian Federation, S.E.Goltsov@yandex.ru

Abstract. Currently, the legal science has not reflected the tactical conditions and techniques for collecting criminally significant voice information on electronic media and in user equipment, in particular, to ensure its safety at the preparatory stage of the inspection of the scene, objects, search. The article reveals the above-mentioned conditions.

Keywords: voice information, electronic media, user equipment, scene inspection, inspection, search

For citation: Goltsov S.E. Takticheskiye usloviya obespecheniya sokhrannosti kriminalisticheski znachimoy golosovoy informatsii pri osmotre mesta proisshestviya, predmetov, obyska [Tactical conditions for ensuring the safety of criminally significant voice information during the inspection of the scene, objects, search]. Kriminalistika: vchera segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 36, no. 4, pp. 46–52 (in Russ.).

Введение

В ходе интервьюирования следователей системы МВД России автором было установлено, что наиболее распространенными следственными действиями, направленными на обнаружение, фиксацию и изъятие электронных носителей и пользовательского оборудования, потенциально содержащих криминалистически значимую голосовую информацию, являются осмотр места происшествия, осмотр, обыск.

Для каждого источника хранения голосовой информации, в том числе электронных носителей и пользовательского оборудования, характерны свои технические особенности, от которых зависит порядок ее получения. Действия на определенных этапах производства осмотра места происшествия, предметов, обыска, используемые при этом тактические приемы зависят от вида носителя голосовой информации.

Особенности криминалистически значимой голосовой информации обусловливают перечень тактических задач, возникающих в процессе ее обнаружения, фиксации и изъятия.

К числу таких задач на подготовительном этапе вышеуказанных следственных действий, направленных на обнаружение, фиксацию и изъятие указанной информации на электронных носителях является обеспечение ее сохранности, которое создаст условия безопасности и защиты ее от уничтожения, модификации и других вредоносных действий.

Основная часть

Эффективное решение указанной тактической задачи требует соблюдения следующих тактических условий:

1. Предварительный анализ сведений, полученных в ходе иных следственных и процессуальных действий, а также от органов, осуществляющих ОРД, включая наличие информации об электронных носителях и пользовательского оборудования, предположительно содержащих голосовую информацию, потенциально имеющую доказательственное значение.

2. Учет обладания подозреваемыми и обвиняемыми компетенциями в области информационно-телекоммуникационных технологий, что будет содействовать ее целенаправленному поиску. Такие лица могут: использовать шифрование данных (например, VeraCrypt, BitLocker), скрытые разделы на жестких дисках; хранить голосовую информацию в облачных хранилищах (Google Drive, Dropbox, Mega и др.) с двухфакторной аутентификацией, на микрокартах памяти (microSD), вшитых в предметы (часы, ручки, обувь и др.), в устройствах IoT – интернет вещей (умных колонках, видеокамерах, роутерах и др.), на носителях с физическими повреждениями, имитирующими неисправность, в USB-устройствах с функцией «Rubber Ducky», маскирующихся под клавиатуру и автоматически вводящих команды; применять стеганографию для сокрытия голосовых сообщений в изображениях, приложениях и других файлах, не предназначенных для ее хранения и передачи.

3. Получение сведений об обстановке на месте производства следственного действия, включая сведения о типе и размерах компьютерного оборудования, его количестве и физических характеристиках. Кроме того, персональные компьютеры могут быть соединены между собой локальной сетью и иметь доступ к информационно-телекоммуникационной сети Интернет посредством подключения с помощью медного кабеля (витой пары) или волоконно-оптической линии

связи, либо соединения с роутером (WiFi). Значение имеет наличие на месте производства следственного действия источников электромагнитного излучения. Проведение осмотра пользовательского оборудования рядом с устройствами и предметами, которые распространяют электромагнитное излучение, может повлечь невозвратимую утрату криминалистически значимой голосовой информации, хранящейся на электронных носителях. Следует получить сведения о имеющихся в месте производства следственного действия технических средств, которые излучают электромагнитные волны. Некоторые авторы считают, что для этого необходимо провести опрос представителей администрации организации, в которой планируется производство соответствующего следственного действия [1, с. 23], но не поясняют, каким образом. В таком случае целесообразно направить поручение органу дознания о получении информации об указанной технической обстановке. Сотрудники, осуществляющие оперативно-розыскную деятельность, с помощью негласных методов и средств получают указанные сведения, в том числе посредством негласного опроса.

4. Привлечение к производству следственного действия участников, обладающих компетенциями в сфере расследования преступлений с использованием информационно-телекоммуникационных технологий, в том числе понятых, обладающих познаниями в указанной сфере, специалистов по сетевым технологиям, по системам электросвязи. По возможности приглашать в качестве специалистов к участию в следственном действии экспертов МВД России, занимающихся производством судебных компьютерных экспертиз.

5. Инструктаж участников следственно-оперативной группы о последовательности действий и выполняемых ими задач: специалист – единственный, кто должен совершать действия, направленные на получение криминалистически значимой голосовой информации, находящейся на электронных носителях в пользовательском оборудовании. Оперативные сотрудники обязаны не допускать кого-либо для контакта с ними и не позволять создавать препятствия для получения голосовой информации, для чего следует лишить сотрудников организации, в которой проводится следственное действие, возможности осуществлять действия, направленные на модификацию, сокрытие, уничтожение голосовой информации, содержащейся на электронных носителях, не допускать их к работе с ними. В этих целях их необходимо разместить в другом помещении и, по возможности, изъять у них все электронные носители, устройства, в том числе мобильной связи. Кроме того, в лице инструктирующего, помимо следователя, должен выступать специалист, чтобы обнаруженная голосовая информация на электронных носителях не была утрачена по неосторожности, из-за неквалифицированных действий лиц, участвующих в следственном действии, а также по причине ошибок, совершенных при их обнаружении, фиксации и изъятии.

6. Подготовка криминалистических средств поиска электронных носителей и пользовательского оборудования. К таким средствам относятся нелинейные локаторы «Лорнет», «Orion», «Люкс», «NR», «BWS WH», профессиональные детекторы нелинейных переходов «NR900EM», а также металлоискатели. Они предназначены для обнаружения скрытых жестких дисков, USB-накопителей, SD-карт, звукозаписывающих устройств, выявления технических средств с возможностью удалённого

уничтожения голосовой информации.

7. Сбор и анализ ориентирующей информации, включающий установление наличия у обыскиваемых лиц или в помещении, подлежащем обыску, устройств, способных записывать, хранить или передавать голосовую информацию: мобильные телефоны, диктофоны, голосовые помощники (Alexa, Siri и др.); компьютеры, ноутбуки, планшеты; устройства умного дома с функцией записи (камеры, колонки); облачные аккаунты (Google Drive, iCloud, и др.). Выяснение возможных способов удалённого уничтожения голосовой информации (например, через функцию «Найти iPhone»). Определение мест вероятного хранения электронных носителей и пользовательского оборудования, потенциально содержащих голосовую информацию: сейфы, скрытые отсеки, внешние накопители, microSD и др.

8. Разработка плана тактики обыска, включающего: время и способ (в том числе в случаях, не терпящих отлагательств, с применением специальных средств для разрушения запирающих устройств и конструкций или без них); распределение ролей: кто контролирует действия лиц, в помещении которых осуществляется обыск, кто изымает технику, кто осуществляет видеозапись; определение приоритетных направлений поиска носителей, содержащих голосовую информацию (рабочий стол, спальня, сейф, серверная комната и т. п.).

9. Подготовка технических средств криминалистического копирования голосовой информации: экранирующие сумки для устройств мобильной связи для блокировки возможного дистанционного вмешательства в целях уничтожения голосовой информации; устройства для безопасного копирования голосовой информации; портативные источники питания для аппаратно-программных комплексов, позволяющих получать доступ к пользовательскому оборудованию и анализировать имеющуюся в нем голосовую информацию; фото- и видеокамеры с резервным питанием; комплекты для опечатывания (пломбы, бирки, конверты).

10. Акцент внимания на установленное в пользовательском оборудовании специальное программное обеспечение, запускающее автоматическое уничтожение голосовой информации, а также предотвращающее попытки несанкционированного доступа к нему. К индикаторам работы такого программного обеспечения могут относиться: массовое удаление файлов без действий пользователя; удаление log-файлов, следов активности; изменение системных процессов (например, отключение резервного копирования); неожиданное завершение работы или перезагрузка после определённых событий (например, ввода неправильного пароля, подключения USB-носителя); снижение производительности компьютера при подключении внешних устройств. В случае, если оборудование объединено в единую сеть [2, с. 216], следует учесть, что с ее использованием могут поступить сигналы для уничтожения голосовой информации. Не следует допускать отключения электричества, что может повлечь уничтожение информации в оперативной памяти компьютера.

11. Внезапность [3, с. 513]. Эффект неожиданности проведения обыска и выемки минимизирует возможность уничтожения голосовой информации, содержащейся на электронных носителях и в пользовательском оборудовании, принадлежащих лицам, у которых они изымаются.

12. Одновременность производства указанных следственных действий, если предполагается изъять

несколько единиц электронных носителей и пользовательского оборудования, содержащих голосовую информацию, расположенных в разных местах. По этой причине обыск следует проводить в одно и то же время во всех обнаруженных помещениях, что также снизит риск утраты или уничтожения криминалистически значимой голосовой информации. Некоторые авторы называют подобный обыск групповым [3, с. 569]. Как отмечено выше, персональные компьютеры могут быть подключены в одну единую сеть, для чего необходимо проверить их на наличие соединения с локальными сетями.

13. Использование средств радиоэлектронного подавления, которые предотвращают возможность внешнего вмешательства посредством программ дистанционного доступа через сеть Интернет и мобильную связь, направленных на недопущение приема/передачи голосовой информации, подачу команд на ее передачу с использованием беспроводных компьютерных сетей и сетей мобильной связи.

К современным средствам радиоэлектронного подавления, применяемым МВД России, относится блокиратор сетей связи «ЛГШ-725», представляющий собой устройство, функциональное назначение которого заключается в создании помех для каналов связи между абонентскими устройствами (мобильными телефонами) и базовыми станциями операторов сотовой связи. Применяется для блокировки цифровых каналов передачи данных, работающих по стандартам GSM, Bluetooth и WiFi.

Ключевым эксплуатационным преимуществом «ЛГШ-725» является простота его настройки и применения, не требующая от оператора наличия узкоспециализированных знаний. Отличительной технической особенностью прибора является архитектура с восемью независимыми каналами регулировки выходной мощности для каждого из частотных диапазонов. Данная функция обеспечивает гибкое конфигурирование зоны подавления в строгом соответствии с поставленными тактико-техническими задачами.

Кроме того, могут быть использованы блокираторы ЛГШ-723, ЛГШ-719, ЛГШ-719 Кейс, ЛГШ-701, ЛГШ-716, ЛГШ-718 в зависимости от того, какие именно сети связи необходимо подавить.

14. Достаточность компетенций специалистов и их опыта работы с аппаратно-программными комплексами (далее – АПК):

1) «Мобильный криминалист Эксперт» (разработчик «МКО Системы», Российская Федерация) – позволяет обойти встроенную технологию аппаратного шифрования информации для устройств с операционной системой (далее – ОС) Android. Имеет возможность извлекать голосовую информацию из сервисов обмена мгновенными сообщениями Viber, WhatsApp, Telegram и др., анализировать полученные данные, расшифровывать резервные копии мобильных устройств, в том числе с выключенными и заблокированными. В методах извлечения данных реализованы функции подбора или обхода пароля на блокировку экрана. Функция «Анализ биллингов» позволяет импортировать и анализировать биллинги, полученные от операторов связи в независимости от формата колонок, размера, структуры файла, дающего возможность преобразовать файл в требуемый формат, после чего специалист имеет возможность проанализировать прямые и косвенные связи между звонящими на графе [4, с. 409];

2) АПК Сегмент-С (производитель в РФ ФГУП НИИ «Квант») – поз-

воляет выделять интересующие группы абонентов из трафика базовых приемопередающих станций в определенном месте;

3) PC-3000 Mobile (разработчик ACELab, Российская Федерация) – мобильный АПК, предназначенный для восстановления и (или) извлечения данных, в том числе голосовой информации из мобильных устройств (телефонов, смартфонов, планшетов и др.), где в качестве внутренней памяти применяются твердотельные накопители и микросхемы памяти [5, с. 130]. Позволяет работать с поврежденными устройствами и электронными носителями информации.

Elcomsoft iOS Forensic Toolkit (разработчик ООО «Элкомсофт», Российская Федерация) **–** специализированный продукт для криминалистического исследования устройств Apple на основе iOS (ряд моделей iPhone, iPod Touch, iPad, Apple Watch и Apple TV). Доступны расширения для ОС на базе Windows и Linux. С помощью iOS Forensic Toolkit можно получить полный доступ к информации, хранящейся в поддерживаемых устройствах, включая доступ к расшифрованному образу файловой системы устройства, паролям и иной защищенной информации, включая голосовую [5, с. 130].

Выводы и заключение

Таким образом, соблюдение рассмотренных тактических условий позволит в дальнейшем максимально эффективно решать задачи по поиску электронных носителей и пользовательского оборудования, получению доступа к их содержимому на рабочем этапе, фиксации голосовой информации и изъятию содержащих ее носителей на заключительном этапе осмотра места происшествия, предметов, обыска.

СПИСОК ИСТОЧНИКОВ

1. *Гребенюк, О. А., Жидков, Д. Н., Макарова, Е. Н., Романова, О. Л.* Тактика обнаружения, изъятия и осмотра средств электронных носителей информации и их подготовки для назначения судебных экспертиз: учебно-практическое пособие. Санкт-Петербург: Санкт-Петербургский университет МВД России. 2020. 48 с.

2. *Гаврилин, Ю. В., Пинкевич, Т. В., Мартыненко, Н. Э.* Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий: учебник: в 2 ч; под общ. ред. Ю. В. Гаврилина. Москва: Академия управления МВД России, 2024. Ч. 1. 304 с.

3. *Аверьянова, Т. В., Белкин, Р. С, Корухов, Ю. Г., Россинская, Е .Р.* Криминалистика: учебник. – 4-е изд., перераб. и доп. – Москва: Норма: ИНФРА-М, 2023. – 928 с.

4. Криминалистика: учебник / под ред. Лаврова В.П. Душанбе, 2022. 660 с.

5. *Севастьянов, П. В.* Цифровые технологии фиксации невербальной доказательственной информации: дис. ... канд. юрид. наук. Москва, 2024. 194 с.

REFERENCES

1. *Grebenyuk O.A., Zhidkov D.N., Makarova E.N., Romanova O.L.* Taktika obnaruzheniya, iz"yatiya i osmotra sredstv elektronnyh nositelej informacii i ih podgotovki dlya naznacheniya sudebnyh ekspertiz [Tactics of detection, seizure and inspection of electronic media and their preparation for the appointment of forensic examinations]. Saint Petersburg, 2020, 48 p. (in Russian).

2. *Gavrilin Yu.V., Pinkevich T.V., Martynenko N.E.* Organizaciya protivodejstviya prestupleniyam, sovershaemym s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij [Organization of countering crimes committed using information and telecommunication technologies]. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2024, Part 1, 304 p. (in Russian).

3. *Averyanova T.V., Belkin R.S., Korukhov Yu.G., Rossinskaya E.R.* Kriminalistika [Criminalistics]. Moscow: Norma, 2023, 928 p. (in Russian).

4. Lavrova V.P.(ed.) Kriminalistika [Criminalistics]. Dushanbe, 2022, 660 p. (in Russian).

5. *Sevastyanov P.V.* Cifrovye tekhnologii fiksacii neverbal'noj dokazatel'stvennoj informacii: dis. ... kand. yurid. nauk. [Digital technologies of fixation of non-verbal evidentiary information: dissertation of the candidate. jurid. sciences']. Moscow, 2024, 194 p. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Гольцов Степан Евгеньевич, преподаватель кафедры уголовного процесса. Барнаульский юридический институт МВД России, 656038, Российская Федерация, г. Барнаул, ул. Чкалова, 49.

INFORMATION ABOUT THE AUTHOR

Stepan E. Goltsov, Lecturer of the Department of Criminal Procedure. Barnaul Law Institute of the MIA of the Russian Federation. 49, Chkalova st., Barnaul, Russian Federation, 656038.