

Е. Н. Митина

*курсант 4 курса факультета правоохранительной деятельности
Белгородского юридического института МВД России
имени И. Д. Путилина*

*Научный руководитель: **Е. А. Новикова**,
профессор кафедры уголовного процесса
Белгородского юридического института МВД России
имени И. Д. Путилина,
кандидат юридических наук*

К ВОПРОСУ О ПРОЦЕССУАЛЬНЫХ ОСОБЕННОСТЯХ ИЗЪЯТИЯ ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ИТ-ПРЕСТУПЛЕНИЙ

Развитие информационных технологий способствует активному распространению применения электронных форм осуществления противоправной деятельности. Многие виды преступлений, к примеру, мошенничество, незаконный оборот наркотиков часто переходят на ИТ-платформу. По данным расширенного заседания коллегии МВД, в марте 2023 г. Президент Российской Федерации Владимир Путин отметил, что «преступления в ИТ-сфере превысили около полумиллиона, составив четверть от всех уголовных правонарушений в России в 2022 году» [1]. Таким образом, В. В. Путин подчеркнул, что противодействие ИТ-преступлениям считается одним из безусловных приоритетов работы всей системы МВД России.

В настоящее время очень остро стоит вопрос по раскрытию и расследованию противоправных деяний, затрагивающих посягательство на компьютерную информацию. В связи с этим возникают процессуальные и организационные проблемы при производстве осмотра места происшествия, осмотра компьютерных и мобильных устройств, а также предметов и документов. Следовательно, наиболее актуальным вопросом при расследовании таких преступлений является отсутствие должной регламентации процесса изъятия значимой информации из интернет-ресурсов. Имеющиеся в законодательстве пробелы и отсутствие методических рекомендаций (алгоритма действий) затрудняют определения практическими сотрудниками процессуальных способов изъятия в конкретной следственной ситуации. Кроме того, процедура изъятия электронных ресурсов не отличается процессуальным единообразием.

Актуальность заявленной тематики связана с необходимостью комплексного изучения процессуальных вопросов изъятия цифровых следов и обусловлена ростом преступлений, совершенных с использованием ИТ-технологий или в сфере компьютерной информации (так, по данным МВД России, в 2023 г.

в стране зарегистрировано 677 тыс. IT-преступлений, на треть больше, чем в 2022 г. (522,1 тыс. таких преступлений) [2].

Существенное значение на стадиях досудебного производства имеет осмотр предметов и документов, электронных носителей информации. Судебная практика по извлечению информации с мобильных телефонов и сайтов демонстрирует несколько способов изъятия информационных данных:

1. Следственные осмотры (в уголовном деле гражданина С., обвиняемого в совершении преступления, предусмотренного ч. 2 ст. 273 Уголовного кодекса Российской Федерации (далее — УК), осмотр мобильного телефона был оформлен как протокол осмотра предметов, в ходе которого была получена информация, подтверждающая причастность гражданина С. к созданию и распространению вредоносной компьютерной программы [3]).

2. Обыск и выемка (так, при проведении обыска по месту жительства вышеупомянутого гражданина С. специалистом в ноутбуке было обнаружено приложение Telegram, открывшееся под учетной записью MrDemiurg, где содержался диалог с пользователем о продаже программного обеспечения, позволявшего осуществлять неправомерный доступ к интернет-сайтам с целью копирования информации [3]).

3. Личный досмотр (в ходе его проведения в отношении Иванова Г. В., обвиняемого в совершении преступлений, предусмотренных ч. 3 ст. 30, пп. «а, г» ч. 4 ст. 228.1, ч. 2 ст. 228, ч. 3 ст. 30, пп. «а, г» ч. 4 ст. 228.1 УК, были обнаружены и изъяты вещество, являющееся смесью, содержащей производное N-метилэфедрона — наркотическое средство общей массой 2,402 г, и каннабис (марихуана) — наркотическое средство массой 0,541 г в высушенном состоянии [4]).

4. Оперативно-розыскные мероприятия (Колесин А. Э., обвиняемый в совершении преступлений, предусмотренных ч. 2 ст. 273, ч. 2 ст. 272 УК, сбыл Свидетелю № 1, действовавшему в рамках оперативно-розыскного мероприятия «проверочная закупка», за п рублей смарт-карту, в которой содержалась компьютерная информация, позволяющая осуществлять несанкционированный доступ к информации [5]).

Как уже отмечалось, изменение современных реалий, ускоренное развитие научно-технического прогресса, активное внедрение информационных технологий неизбежно приводят к совершенствованию криминалистической техники при проведении осмотра и выемки предметов и документов. Так, цифровые носители информации и сотовые устройства становятся новыми объектами осмотра. В связи с этим необходимо разрабатывать новые методики и вводить дополнительные нормы в уголовно-процессуальное законодательство. Таким образом, предлагаем данный вид осмотра при расследовании киберпреступлений законодательно закрепить в ч. 1 ст. 144 Уголовно-процессуального кодекса

Российской Федерации (далее — УПК), а именно информацию о существовании этого вида осмотра, именуемого как осмотр сетевых информационных ресурсов, а также основания и порядок его проведения.

Изъятое техническое устройство будет являться вещественным доказательством, а содержащаяся на нем информация — электронной, то есть электронным доказательством. Общий порядок изъятия электронных носителей информации и копирования с них информации закреплен в ст. 164.1 УПК. Также для изъятия электронных следов с мобильного устройства может быть назначена судебная компьютерно-техническая экспертиза (ст. 195, 283 УПК). Обратим внимание, что Конституционный Суд Российской Федерации разъясняет, что «проведение осмотра и экспертизы с целью получения информации, находящейся в электронной памяти устройств, изъятых при производстве следственных действий, не предполагает вынесения об этом специального судебного решения» (определение от 24 июня 2021 г. № 1364-О) [6].

Решение задач, связанных с изучением внутреннего информационного поля смартфона, относится к компетенции судебной компьютерно-технической экспертизы, в частности, следующих ее видов: программно-компьютерной, информационно-компьютерной экспертизы данных, компьютерно-сетевой [7, с. 68]. Выделим одну из проблем при извлечении информационного содержимого из мобильных устройств. Так, отмечается высокий риск повреждения микросхемы памяти, что говорит о необходимости регулирования последствий, наступающих при причинении имущественного вреда гражданам в результате производства экспертизы. В данном случае ответчиком возмещения материального ущерба в размере стоимости мобильного телефона будут ведомства, проводившие экспертизу.

Отметим, существует процессуальная неурегулированность вопроса, связанного с разъяснением лицам, у которых изымаются телефоны, наличия риска повреждения их устройств или их свойств, которые могут быть утрачены при производстве компьютерных экспертиз. Необходимо включить данное положение в общий перечень при оформлении изъятия смартфона в протоколе.

В заключение дополним, что в практической деятельности в части процессуального обеспечения привлечения специалистов при изъятии цифровых следов следователями, дознавателями выносятся постановления о привлечении специалистов и письмо в Экспертно-криминологический центр МВД Российской Федерации (далее — ЭКЦ). Так, по уголовному делу о преступлениях, предусмотренных ч. 4 ст. 159; ч. 3 ст. 30, ч. 4 ст. 159 УК, были запланированы к проведению обыски и иные процессуальные действия, связанные с обнаружением электронных носителей информации, на территории г. Белгорода и Белгородского района. В связи с этим следователем вынесено постановление о привлечении специалистов для оказания содействия в отыскании,

обнаружении, закреплении следов преступления, изъятии и осмотре электронных носителей информации, применении технических средств и письмо в адрес начальника ЭКЦ УМВД России по Белгородской области.

Таким образом, существует несколько способов изъятия цифровых следов органами предварительного расследования. В случае производства следственного осмотра необходима процессуальная регламентация видов осмотра в УПК, оснований его проведения, оформления протокола осмотра сетевых информационных ресурсов при привлечении специалистов — направление постановления об их привлечении и письма в ЭКЦ для оказания содействия, а также закрепления в протоколах изъятия мобильных устройств уведомления собственника о возможном риске потери информации и работоспособности смартфона с последующим возмещением средств с ведомства, проводившего экспертизу. Должная нормативная регламентация способствует систематизации процессуальных и организационных аспектов изъятия информации с цифровых, мобильных устройств и ресурсов.

1. Число киберпреступлений в России [Электронный ресурс] // TADVISER : [сайт]. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России?ysclid=ljmwcf7061846100936 (дата обращения: 26.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
2. МВД РФ: в 2023 году в стране зарегистрировано рекордное количество IT-преступлений [Электронный ресурс] // HABR : [сайт]. URL: <https://habr.com/ru/news/796013/> (дата обращения: 26.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
3. Дело № 1-207/2022 [Электронный ресурс] // Судебные решения РФ : [сайт]. URL: <https://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/70251361/extended> (дата обращения: 27.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
4. Дело № 1-237/2023 [Электронный ресурс] // Судебные решения РФ : [сайт]. URL: <https://судебныерешения.рф/75702893> (дата обращения: 26.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
5. Дело № 1-110/2022 [Электронный ресурс] // Судебные решения РФ : [сайт]. URL: <https://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/69705990/extended> (дата обращения: 27.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
6. Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации [Электронный ресурс] : определение Конституц. Суда Рос. Федерации, 24 июня 2021 г., № 1364-О. URL: <https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-24062021-n-1364-o/?ysclid=lu9lmwd1qz590661119> (дата обращения: 26.03.2024). [Перейти к источнику](#) [Вернуться к статье](#)
7. Жижина М. Извлечение данных с мобильных телефонов: проблемы на практике // Уголовный процесс. 2024. № 3. С. 66–71. [Вернуться к статье](#)