DOI: 10.17803/1729-5920.2021.178.9.102-118

Е. Р. Россинская*,
И. А. Рядовский**

Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика[1]

Аннотация. В статье рассмотрено учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий, входящее в систему частной теории информационно-компьютерного обеспечения криминалистической деятельности. Предмет учения составляют закономерности собирания, исследования и использования компьютерной информации при производстве следственных и судебных действий, объектами являются тактика и технология следственных и судебных действий. На теоретической основе этого учения разработаны тактика и технология невербальных следственных действий по делам о компьютерных преступлениях: осмотра места происшествия, обыска, выемки, следственного эксперимента с учетом выбора тактического воздействия и принятия тактического решения в зависимости от специфики следственных ситуаций в условиях тактического риска, связанного с возможным противодействием расследованию. Тактико-технологическое обеспечение производства вышеназванных невербальных следственных действий разработано с учетом особенностей цифровых следов, которые характеризуются высокой скоростью трансформации, легко уничтожаются и модифицируются, могут быть представлены практически бесконечным количеством копий, отличаются невозможностью восприятия непосредственно органами чувств, а воспринимаются только с использованием специальных устройств и программ по обнаружению, фиксации и обеспечению сохранности, подтверждаются контрольными числами (хеш-суммами) либо иными данными, свидетельствующими об их целостности. Определены основные принципы работы с цифровыми следами при производстве невербальных следственных действий: сохранность в неизменном виде цифровых следов на всех этапах работы с ними; полное отражение в протоколах следственных действий всех манипуляций; исключительная важность подготовительных мероприятий, включающих выбор специалиста и определение его компетенции, наличие необходимого оборудования и программного обеспечения для работы с цифровыми следами. Для каждого из вышеназванных следственных действий при расследовании компьютерных преступлений разработаны тактические приемы и технологическое обеспечение наиболее результативного получения криминалистически значимой доказательственной и розыскной информации.

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003.

* *Россинская Елена Рафаиловна,* доктор юридических наук, профессор, директор Института судебных экспертиз, заведующий кафедрой судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), заслуженный деятельно науки РФ, почетный работник высшего профессионального образования РФ
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
elena.rossinskaya@gmail.com

** *Рядовский Игорь Анатольевич,* заместитель руководителя юридического департамента — руководитель отдела расследования компьютерных инцидентов АО «Лаборатория Касперского»
Ленинградское ш., д. 39а, стр. 2, г. Москва, Россия, 125212
RyadIA@yandex.ru

Ключевые слова: компьютерные преступления; компьютерные средства и системы; цифровой след; хеш-сумма; информационно-компьютерное обеспечение криминалистической деятельности; невербальные следственные действия; тактико-технологическое обеспечение осмотра места происшествия, обыска, выемки, следственного эксперимента.
Для цитирования: *Россинская Е. Р., Рядовский И. А.* Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex russica. — 2021. — Т. 74. — № 9. — С. 102–118. — DOI: 10.17803/1729-5920.2021.178.9.102-118.

Tactics and Technology of Non-Verbal Investigative Actions Production in Computer Crimes Cases: Theory and Practice[2]

Elena R. Rossinskaya, Dr. Sci. (Law), Professor, Director of the Forensic Examination Institute, Head of the Department of Forensic Examination, Kutafin Moscow State Law University (MSAL), Honored Scientist of Russia, Honorary Worker of Higher Professional Education of the Russian Federation
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
elena.rossinskaya@gmail.com

Igor A. Ryadovskiy, Deputy Head of the Legal Department, Head of the Computer Incident Investigation Department, Kaspersky Lab JSC
Leningradskoe sh., 39a, p. 2, Moscow, Russia, 125212
RyadIA@yandex.ru

Abstract. The paper considers the doctrine of information and computer forensic support of investigative and judicial actions tactics, which is part of the system of the private theory of information and computer support of forensic activity. The subject of the teaching is the laws of gathering, scrutinizing and applying computer information in the production of investigative and judicial actions. The objects are the tactics and technology of investigative and judicial actions. Based on the theoretical aspects of the teaching, the authors have developed the tactics and technology of non-verbal investigative actions in cases of computer crimes. Among these are inspection of the scene of the crime, search, seizure, investigative experiment, given the choice of tactical impact and making a tactical decision depending on the specifics of investigative situations in the conditions of tactical risk associated with possible counteraction to the investigation. The tactical and technological support for the production of the above-mentioned non-verbal investigative actions is developed taking into account the features of digital traces, which are characterized by a high speed of transformation, are easily destroyed and modified, can be represented by an almost infinite number of copies, are characterized by the impossibility of perception directly by the senses, but only with the use of special devices and programs for detection, fixation and preservation, are confirmed by control numbers (hash sums) or other data indicating their integrity. The basic principles of working with digital traces in the production of non-verbal investigative actions are determined. They are the preservation of digital traces unchanged at all stages of working with them; full reflection of all manipulations in the protocols of investigative actions; the exceptional importance of preparatory measures, including the selection of a specialist and the determination of his competence, the availability of the necessary equipment and software for working with digital traces. For each of the above-mentioned investigative actions in the investigation of computer crimes, tactical techniques and technological support for the most effective obtaining of criminally significant evidentiary and investigative information have been developed.
Keywords: computer crimes; computer tools and systems; digital footprint; hash sum; information and computer support for forensic activities; non-verbal investigative actions; tactical and technological support for the inspection of the scene of the crime, search, seizure, investigative experiment.
Cite as: Rossinskaya ER, Ryadovskiy IA. Taktika i tekhnologiya proizvodstva neverbalnykh sledstvennykh deystviy po delam o kompyuternykh prestupleniyakh: teoriya i praktika [Tactics and Technology of Non-Verbal Investigative Actions Production in Computer Crimes Cases: Theory and Practice]. *Lex russica*. 2021;74(9):102-118. DOI: 10.17803/1729-5920.2021.178.9.102-118. (In Russ., abstract in Eng.).

[2] The reported study was funded by RFBR according to the research project № 18-29-16003.

Глобальный процесс цифровизации всех сторон жизни человека, общества и государства, взрывное развитие информационно-коммуникационных технологий ожидаемо привели к востребованности новых технологий и преступным сообществом, что породило такой негативный социальный феномен, как киберпреступность. Ответом явилось инновационное развитие криминалистической науки, отвечающее современным потребностям раскрытия и расследования компьютерных преступлений. Следует подчеркнуть, что дефиниция «компьютерное преступление» давно уже применяется в криминалистическом аспекте и связана не с уголовно-правовой квалификацией деяния, а со способом преступления и, соответственно, с методикой его раскрытия и расследования[3]. Поэтому к компьютерным преступлениям (киберпреступлениям) относятся не только преступления, объектом которых выступают общественные отношения в сфере обработки, хранения и передачи компьютерной информации (так называемые киберзависимые преступления), а любые преступные посягательства, совершаемые с применением информационно-коммуникационных технологий (ИКТ)[4].

Для теоретического и прикладного обеспечения раскрытия и расследования компьютерных преступлений нами разрабатывается частная теория информационно-компьютерного обеспечения криминалистической деятельности, предметом которой являются закономерности возникновения, движения, собирания и исследования компьютерной информации при расследовании преступлений и судебном рассмотрении уголовных дел, а объектами — с одной стороны, сами компьютерные средства и системы как носители розыскной и доказательственной криминалистически значимой информации, с другой — система действий и отношений в механизмах преступлений с использованием компьютерных средств и систем, а также криминалистических компьютерных технологий собирания, исследования и использования криминалистически значимой доказательственной и ориентирующей информации. В систему этой теории информационно входит целый ряд учений[5], одним из которых является учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий. Его предметом являются закономерности собирания, исследования и использования компьютерной информации при производстве следственных и судебных действий, в первую очередь по уголовным делам, а также судебных действий по гражданским и административным делам. Объектом учения является сама тактика и технология следственных и судебных действий с учетом следственных и судебных ситуаций, обусловливающих выбор тактического воздействия и принятия тактического решения в условиях тактического риска[6].

В зависимости от формы познания, которая преимущественно используется при их проведении, следственные действия условно подразделяют на вербальные, невербальные и смешанные[7]. Для расследования компьютерных преступлений наиболее характерными невербальными следственными действиями являются осмотр места происшествия, осмотр предметов, обыск, выемка и следственный эксперимент.

Одновременно с развитием информационно-коммуникационных технологий возрастает многообразие объектов, предназначенных для поддержания вычислительных процессов: персональные компьютеры, ноутбуки, планшеты, умные часы, смарт-браслеты, смартфоны, бытовые умные устройства — так называемый интернет вещей (IoT), маршрутизаторы, устройства беспроводного доступа, серверы различных типов и видов, в том числе распределенные системы, построенные по принципу

---

3 *Россинская Е. Р.* Криминалистика : учебник для вузов. М. : Норма, 2016. С. 440–442.

4 McGuire and Dowling. Cybercrime: A review of the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes-fraud and theft // URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf (дата обращения: 11.07.2021).

5 *Россинская Е. Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (99). С. 193–202.

6 *Россинская Е. Р.* Направления инновационного развития криминалистической тактики и методик расследования в условиях глобальной цифровизации // II Минские криминалистические чтения : материалы Международной научно-практической конференции (Минск, 10 декабря 2020 г.) : в 2 ч. Минск : Академия МВД Республики Беларусь, 2020. Ч. 1. С. 207–211.

облачных технологий. Все эти устройства предназначены для работы с цифровыми данными. Причем в случае с облачными хранилищами компьютерная информация хранится и обрабатывается уже не в одном месте, а «в нескольких центрах данных в различных географических точках»[8].

При этом осмотр и предварительное исследование средств вычислительной техники, обнаруженных на месте происшествия либо в ходе обыска; информации, хранящейся на удаленных вычислительных ресурсах, в том числе построенных по принципу облачных технологий; цифровых данных, передающихся по компьютерным сетям, значительно расширяют возможности процесса доказывания по уголовным делам, поскольку позволяют собирать криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи и представляющую собой цифровые следы[9]. С криминалистической точки зрения можно говорить об особом виде доказательств — цифровых доказательствах.

По мнению зарубежных ученых-криминалистов, к цифровым доказательствам (англ. digital evidence) относятся данные в любом виде представления, которые можно извлечь из компьютерных систем для использования в доказывании, подтверждения либо опровержения проверяемых фактов и обстоятельств[10].

Близкое по сути определение предлагают и российские криминалисты. Так, по мнению В. Б. Вехова, электронные доказательства — это любые сведения (сообщения, данные), представленные в электронной форме, на основе которых суд, прокурор, следователь, дознаватель в определенном процессуальным законодательством порядке устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по делу, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела[11].

Цифровые следы являются следами материальными, так как, будучи оставленными в результате определенных событий, отражаются на материальных объектах, хотя в некоторых случаях период их существования весьма невелик. По происхождению цифровые следы являются технологическими, поскольку формирование данных следов обусловлено спецификой реализации информационных технологий. Информационная составляющая становится доступной для восприятия только после их интерпретации с помощью прикладного программного обеспечения и с использованием средств вывода[12]. Поэтому в процессе поиска и изъятия цифровых следов следователь практически не использует чувственную форму познания. Собирание цифровых следов производится в процессе невербальных следственных действий с применением специальных криминалистических систем, предназначенных для их поиска и обработки, иного программного обеспечения и средств вычислительной техники, приспособленных для решения этой задачи. С учетом этого при проведении невербальных следственных действий требуется обязательное применение специальных технических средств, что обусловливает многократно возрастающую роль специалиста и требований, предъявляемых к его компетенции[13].

В ходе невербальных следственных действий грамотно организованная работа по

---

7 *Россинский С. Б.* Следственные действия : монография. М. : Норма, 2018. С. 70–71.

8 Introduction to Cybercrime. United Nations Office on Drugs and Crime // URL: https://www.unodc.org/e4j/en/tertiary/cybercrime.html (дата обращения: 11.07.2021).

9 *Россинская Е. Р.*, *Семикаленова А. И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. 2020. Т. 11. Вып. 3 : Право. С. 745–759.

10 *Maras M.-H*. Cybercriminology. Oxford University Press, 2016. P. 44.

11 *Вехов В. Б.* Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 46–50.

12 *Россинская Е. Р.*, *Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы : Алматинская академия МВД Республики Казахстан, 2019. С. 6–9.

13 *Рядовский И. А.* Компетенции специалиста по работе с цифровыми следами при производстве следственных действий // Законы России. Опыт. Анализ. Практика. 2020. № 9. С. 94–100.

поиску, обнаружению и предварительному исследованию цифровых следов, имеющих криминалистическое значение, позволяет непосредственно на месте получить сведения о способах преступления, обнаружить, зафиксировать и изъять методом консервирования на электронном носителе информации эти цифровые следы, выявить иные обстоятельства происшествия. Это исключительно важно, поскольку большинство компьютерных преступлений совершается в условиях неочевидности, когда потерпевший сталкивается с наступившими в результате совершенного деяния негативными последствиями, например с утечкой конфиденциальной информации либо несанкционированным списанием денежных средств со своего банковского счета, но ни способ преступления, ни преступник не известны. В этом случае формальный подход к следственному действию может повлечь безвозвратную утрату доказательственной информации, что обусловлено в первую очередь такими свойствами цифровых следов, как высокая скорость модификации в вычислительных системах, а также возможность их уничтожения либо фальсификации с целью сокрытия преступления.

Международный опыт по регламентации работы с цифровыми следами преступления подтверждает значимость этой проблемы. Так, в 2012 г. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) опубликовали международные стандарты, касающиеся обращения с цифровыми доказательствами[14]. В 2014 г. для добровольного применения был утвержден национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме», идентичный указанному международному стандарту ИСО и МЭК[15].

Стандартом предусмотрены четыре этапа обращения со свидетельствами, представленными в цифровой форме: идентификация, сбор, получение, сохранение. Рассмотрим эти этапы подробнее.

В ходе этапа идентификации производится выявление средств вычислительной техники, электронных носителей информации и иных устройств, которые могут содержать цифровые следы преступления либо иную криминалистически значимую информацию. Одновременно проводится анализ на предмет определения приоритетов в изучении устройств с учетом степени риска утраты хранящейся на них информации. Например, данные, содержащиеся в оперативной памяти работающего компьютера, характеризуются высокой степенью волатильности, в то время как состояние данных, хранящихся на внешнем энергонезависимом электронном носителе информации, не подключенном к компьютеру, стабильно. Но если такой носитель информации подключен к работающей компьютерной системе, неверное определение очередности работы с обнаруженными на месте следственного действия объектами может привести к утрате доказательств при отключении электронного носителя информации от компьютера либо вследствие обесточивания компьютера в том случае, если данные на носителе информации были зашифрованы.

На следующем этапе сбора принимается решение об изъятии обнаруженных объектов для последующего осмотра либо проведения экспертизы. На такое решение могут влиять различные факторы. Например, как было указано выше, выключение работающего компьютера для изъятия приведет к потере информации, содержащейся в оперативной памяти, либо к утрате доступа к зашифрованным данным на носителях информации. В то же время изъятию средств вычислительной техники могут препятствовать иные обстоятельства, такие как недопустимость приостановления непрерывного производственного процесса.

Собирание цифровых следов — дальнейший этап работы с данными. Как авторы уже неоднократно отмечали, основной криминалистический принцип при работе с компьютерной техникой и электронными носителями информации — сохранение в неизменном виде хранящихся на них цифровых следов. При невозможности следования этому правилу,

[14] ISO/IEC 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence // URL: https://www.iso.org/ru/standard/44381.html (дата обращения: 11.07.2021).

[15] ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме // URL: http://docs.cntd.ru/document/1200112857 (дата обращения: 11.07.2021).

например при необходимости осмотреть работающую систему, действия по манипуляции с данными должны быть строго выверены и отображены в протоколе. В иных случаях исследование информационных объектов производится посредством осмотра их копий, созданных с использованием специальных криминалистических средств — копировщиков и блокираторов, исключающих возможность внесения изменений в информацию, хранящуюся на изъятых компьютерах и носителях[16].

Современные дубликаторы, помимо обеспечения безопасного процесса копирования информации, обладают рядом дополнительных возможностей, реализующих криминалистическую составляющую их функциональности, а именно: возможность верифицировать созданную копию и документировать результаты основных этапов работы в отдельный файл, в том числе фиксировать основные характеристики диска-источника, включая его модель и серийный номер, дату и время создания копии, контрольную сумму (хеш-сумму) образа диска.

Еще один криминалистический принцип при работе с цифровыми следами, на необходимость соблюдения которого прямо указано в стандарте ISO/IEC 27037, — это четкое и полное отражение в протоколе манипуляций, производимых как с осматриваемыми физическими объектами (средствами вычислительной техники, электронными носителями информации), так и непосредственно с объектами информационными. Так, при случайном включении мобильного телефона данный факт регистрируется в журнале событий операционной системы устройства. Для обычного пользователя эта информация недоступна, однако при углубленном исследовании устройства с использованием специальных криминалистических средств данное событие будет выявлено и, в случае если оно не было отражено в протоколе, может рассматриваться как несанкционированный доступ к компьютерной информации, что, свою очередь, может повлечь признание результатов последующих осмотров данной техники недостоверными, а проведенных судебных экспертиз — недопустимыми доказательствами.

Если изготовление образов (побитовых копий) дисков невозможно, например приходится осматривать работающую компьютерную систему либо размер диска слишком большой, а время ограничено, допустимо копирование значимых для расследования данных на логическом уровне, то есть файлов и папок либо содержимого адресного пространства диска. Учитывая, что при работе с цифровыми следами в активной функционирующей системе невозможно обеспечить неизменность информации, все манипуляции, связанные с поиском, изучением и копированием криминалистически значимой информации, также должны быть детально задокументированы, а в протоколе необходимо указать причины, которые повлияли на принятие такого решения.

На заключительном этапе — сохранения — обеспечивается сохранность полученных цифровых следов и средств вычислительной техники, в которых они могут содержаться. Особенность этого этапа в том, что он распространяется на все предыдущие этапы, начиная с идентификации, и на любые последующие исследования изъятой компьютерной техники и цифровых следов с целью предупреждения их повреждения и фальсификации.

Анализируя рассмотренные положения международного стандарта ISO/IEC 27037, можно констатировать, что рекомендации, изложенные в нем, логичны и разумны и могут быть адаптированы для национальных процессуальных законодательств. При этом необходимо отметить, что отечественное уголовно-процессуальное законодательство по большей части в процедурном плане может обеспечить соблюдение технических рекомендаций по обращению с цифровыми следами в ходе невербальных следственных действий. Так, ч. 2 ст. 164.1 УПК РФ предусмотрено обязательное участие специалиста в следственных действиях, в ходе которых производится изъятие электронных носителей информации. Тем самым, с одной стороны, обеспечивается выполнение рекомендаций относительно привлечения к работе с цифровыми следами компетентного технического специалиста, а с другой — выполняется требование о детальном документировании манипуляций, произведенных с цифровыми устройствами и объектами.

Таким образом, при производстве невербальных следственных действий, в ходе которых осуществляется работа с цифровыми сле-

[16] *Чекунов И. Г.*, *Голованов С. Ю.* [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие. 2-е изд. / под ред. И. Г. Чекунова. М. : Московский университет МВД России имени В. Я. Кикотя, 2019. С. 94.

дами, важно соблюдать следующие правила: обеспечивать неизменность цифровых следов, хранящихся на осматриваемых устройствах; для поиска, изучения, изъятия и иных манипуляций с цифровыми следами привлекать специалиста, имеющего соответствующую подготовку; документировать в полном объеме действия по изъятию, хранению и передаче цифровых следов, доступу к ним и, соответственно, к устройствам, на которых они содержатся, обеспечивать их защиту и доступность для дальнейших судебных исследований.

Следует особо отметить значимость подготовительных мероприятий при проведении невербальных следственных действий для дел данной категории. Разумеется, подготовка обязательна при проведении любого следственного действия, однако отсутствие приготовительных мероприятий либо формальный подход к их проведению именно по делам о компьютерных преступлениях может повлечь наибольший ущерб для расследования, выражающийся в утрате возможностей для сбора доказательств. Поэтому на этапе подготовки следователю требуется подыскать и привлечь к проведению следственного действия соответствующего специалиста, убедиться в его компетентности, после чего совместно с ним уточнить обстоятельства дела, заранее собрать сведения о дате и времени совершения преступления, местонахождении скомпрометированной компьютерной системы, моделях и характеристиках вычислительных устройств, емкости их жестких дисков, сетевом окружении и т. п. Затем надлежит проверить наличие необходимого оборудования и программного обеспечения для работы специалиста с цифровыми следами. Помимо специальных криминалистических средств, в перечень которых входят в том числе программы для снятия снимка оперативной памяти, блокираторы для исследования компьютерной техники, копировщики для копирования жестких дисков, при производстве невербальных следственных действий могут понадобиться переходники и кабели, электронные носители информации для консервирования компьютерных данных, латексные перчатки и иные средства защиты, необходимые для предотвращения оставления специалистом каких-либо следов на осматриваемой технике, специальный упаковочный материал, служащий для безопасного перемещения и хранения компьютерной техники и электронных носителей информации, материал для маркировки портов и кабелей в случае изъятия всех элементов компьютерной сети.

Невербальные следственные действия проводятся с целью поиска, фиксации и изъятия цифровых следов преступления, которые могут быть обнаружены в местах автоматизированной обработки, хранения и передачи данных с использованием вычислительных мощностей:

— рабочее место преступника (компьютерные устройства, электронные носители информации, средства связи, записи);
— место происшествия (компьютерная система);
— сетевые ресурсы преступника (в локальной сети);
— сетевые ресурсы преступника (в глобальной сети);
— каналы связи преступника (сетевой трафик);
— легальные сетевые ресурсы, используемые в преступной деятельности (почтовые серверы, вычислительные мощности провайдеров хостинга, ресурсы провайдера по предоставлению доступа в Интернет и т. п.).

Наиболее распространенное и значимое невербальное следственное действие для расследования компьютерных преступлений — осмотр места происшествия. Сложность этого следственного действия, помимо прочего, обусловлена его неотложностью, обычно по горячим следам совершенного преступления, что оставляет крайне мало времени для подготовки. Тем не менее определенные подготовительные мероприятия провести необходимо, иначе, прибыв на место происшествия для его осмотра с целью поиска, фиксации и изъятия следов преступления и других вещественных доказательств, выяснения обстановки и иных обстоятельств, имеющих значение для дела, следователь зачастую сталкивается с проблемной ситуацией, поскольку не обнаруживает видимых материальных признаков совершенного деяния. Жилые или офисные помещения, порядок в которых не нарушен, с находящимися в них средствами вычислительной техники (компьютеры, мобильные устройства, серверы, маршрутизаторы), в ряде случаев связаны в локальную сеть и размещены в разных частях здания. Установление связи между преступлением и осматриваемым местом происшествия при таких обстоятельствах возможно только с использованием специальных знаний и применением криминалистических технических средств.

В самом общем виде можно определить следующий порядок действий при осмотре средств вычислительной техники:

— внешний осмотр компьютерной техники;
— проверка наличия активных сетевых подключений;
— осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов);
— снятие копии (дампа) содержимого оперативной памяти;
— выключение компьютера и создание копии жесткого диска;
— отсоединение кабелей и внешних устройств (в случае изъятия взаимосвязанных объектов необходимо промаркировать имеющиеся кабельные соединения);
— составление протокола и упаковка изъятого.

Тактические особенности осмотра места происшествия, сопряженного с работой с цифровыми устройствами и данными, зависят от конкретных обстоятельств дела. При наличии на месте происшествия одного компьютера следователь в полной мере может контролировать полноту, активность, методичность и последовательность осмотра, а роль специалиста носит технический характер и заключается в выполнении определенного набора действий, выбор которых обычно зависит от того, включен или выключен компьютер на момент проведения осмотра. В случае с неработающей системой сначала производится внешний осмотр компьютерной техники, отсоединение кабелей и внешних устройств, их упаковка (в случае изъятия взаимосвязанных объектов необходимо предварительно отметить, к какому порту что подключено) либо, при наличии оснований, может быть изъят не компьютер целиком, а создана побитовая копия его жесткого диска, которая изымается и приобщается к уголовному делу. Если же система активна, то перед ее выключением и созданием копии диска дополнительно проводится проверка наличия активных сетевых подключений, выполняется осмотр компьютерной информации (установленных и использующихся приложений, файловой системы, запущенных процессов) и снятие копии содержимого оперативной памяти.

Совершенно иначе проводится осмотр компьютерной системы, являющейся локальной сетью, которая включает рабочие станции сотрудников, серверы, в том числе почтовые серверы, прокси-серверы, серверы контроллеров доменов, маршрутизаторы, коммутаторы, кабельную систему. Элементы локальной сети и целые ее сегменты могут быть разнесены не только по разным помещениям в здании, но и по различным географическим регионам, если для построения сети используется технология VPN (от англ. Virtual Private Network — виртуальная частная сеть). Оставив за рамками статьи процессуальные вопросы, что в таком случае считать местом осмотра, отметим очевидный факт: границы места осмотра виртуально раздвигаются, предоставляя больше возможностей для поиска криминалистически значимой информации.

Аналогичная ситуация может возникнуть на месте происшествия в случае, если обнаруженные при осмотре средства вычислительной техники подключены к удаленным хранилищам информации, в том числе к облачным, либо в ходе осмотра помещения провайдера хостинговых услуг, предоставляющего в аренду вычислительные мощности, серверы которого физически размещены в центрах обработки данных (ЦОД) в различных регионах страны. При таких обстоятельствах многократно возрастает роль специалиста: от него требуется уже не выполнение рутинных действий, а творческая вдумчивая работа на протяжении длительного времени, сопровождающаяся значительным психическим напряжением. Достижение результатов осмотра зависит от профессиональной и организационной подготовки специалиста, который вынужден самостоятельно выбирать тактические приемы осмотра места происшествия.

Учитывая огромный размер информации, хранящейся в локальной компьютерной сети, при ее осмотре (например, в связи с проведенной сетевой атакой) тактически наиболее целесообразным видится применение субъективного метода осмотра[17], который выражается в движении по цифровым следам, оставленным в сети, начиная от выявленной скомпрометированной рабочей станции, далее по цепочке других компьютеров и серверов до устройства, с которого началось проникновение, окончившееся получением несанкционированного доступа к системе и его реализацией.

Для поиска и обнаружения цифровых следов преступления могут быть изучены следующие процессы и объекты на компьютерах сети: процессы выполняемых программ; планировщики задач операционной системы; сервисы операционной системы; сетевой трафик; файлы; журнальные файлы событий операционной

[17] *Россинская Е. Р.* Криминалистика : учебник для вузов. М. : Норма, 2016. С. 262–263.

системы и программных систем мониторинга и защиты компьютерной информации.

На основании собранных сведений формируется хронологическая последовательность событий в сети, связанных с получением несанкционированного доступа, и составляется схема развития сетевой атаки, затрагивающей различные элементы локальной сети. При составлении таких схем необходимо обязательно учитывать негативные обстоятельства[18], например изменения в файловой системе, ветках реестра, сведения из журналов событий, которые в силу своего наличия либо, напротив, отсутствия подтверждают или опровергают рассматриваемые следственные версии.

В случае невозможности изъятия средств вычислительной техники и изготовления посекторных копий их дисков вследствие большого размера или непрерывного производственного процесса следует рассмотреть следующие варианты сбора цифровых следов, имеющих значение для расследования уголовного дела:

1. Создание копии логического (а не физического) диска, если размер логического диска несопоставимо меньше неразмеченной области физического диска, например с помощью специальной криминалистической программы — EnCase Forensic Imager.

2. Целевое копирование файлов, если известно, какие именно сведения представляют интерес, а также их расположение в файловой системе осматриваемого устройства.

3. Копирование файлов, содержащих в силу своего назначения достаточно сведений для анализа возможной компрометации устройства либо его использования в противоправных целях, таких как копия (дамп) содержимого оперативной памяти; файл гибернации; страничный файл; ветви реестра операционной системы; журнальные файлы; файл $MFT (Master File Table); файл Prefetch; файл-листинг с хеш-суммами. Если требуется по обстоятельствам дела, копируются файлы, содержащие копии веб-страниц, посещенных с помощью браузеров; файлы, содержащие историю посещения веб-страниц; архив электронной почты; настройки VPN; профили пользователей и т. п.

Если по обстоятельствам дела необходимо производство судебной экспертизы всей компьютерной системы, изъятию подлежат взаимосвязанные объекты, включающие в себя аппаратное, программное и информационное обеспечение и являющиеся составными частями единого информационного технологического процесса.

Обнаруженные в ходе осмотра цифровые следы, которые характеризуются позволяющими их идентифицировать признаками: контрольной суммой (хеш-суммой), рассчитанной по криптографическому алгоритму, размером файла и другими его атрибутами, необходимо сохранить на электронных носителях информации. Сведения о хеш-сумме извлеченных данных и характерных признаках носителя информации, на который они были сохранены, вносятся в протокол. В протоколе также должны быть по́лно и точно отражены ход и результаты проведенного осмотра, наименование примененных специалистом технических и программных средств.

Следует еще раз подчеркнуть важность подготовительного этапа в проведении невербальных следственных действий по делам о компьютерных преступлениях. Формальный подход следователя к проверке наличия необходимых компетенций у специалиста может привести к ситуации, при которой из-за отсутствия у последнего достаточных профессиональных знаний и навыков работы с цифровыми следами будут упущены важные информационные объекты или не сохранены надлежащим образом цифровые следы преступления, что сделает такие доказательства непригодными для использования либо повлечет их утрату[19].

Однако, несмотря важность цифровых следов для установления способа компьютерного преступления, в ходе осмотра места происшествия нельзя сосредотачиваться исключительно на средствах вычислительной техники, игнорируя иные предметы и документы, которые могут нести в себе криминалистически значимую информацию. Так, исходный код вредоносной программы может быть обнаружен в распечатанном либо даже рукописном виде, как и записи, подтверждающие неправомерный доступ к компьютерным системам, пароли к заблокированным компьютерным устройствам, реквизиты доступа к облачным сервисам, схе-

[18] *Белкин Р. С.* Курс криминалистики : учеб. пособие. 3-е изд., доп. М. : Юнити-Дана, Закон и право, 2001. С. 796–799.

[19] *Casey E*. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011. С. 228.

мы сетевой инфраструктуры, используемой при совершении преступлений, и т. п.[20]

Расследуя неправомерный доступ к корпоративной компьютерной системе, следует рассматривать как одну из версий возможную причастность к преступлению сотрудника потерпевшей организации, а значит, может потребоваться осмотр и изъятие записей с видеокамер наблюдения, исследование помещения, где размещены автоматизированные рабочие места, на предмет выявления признаков несанкционированного проникновения, поиск следов рук, оставленных сотрудниками, которым запрещен проход в осматриваемое помещение. Нельзя исключить из списка следственных версий и инсценировку применения вредоносных программ, когда сотрудники потерпевшей организации специально загружают в компьютерную систему вредоносное программное обеспечение, чтобы ввести следствие в заблуждение относительно истинных обстоятельств произошедшего и затруднить установление механизма и способа совершения компьютерного преступления. В другом случае вредоносная программа может быть использована для сокрытия следов иного преступления, например налогового, когда, инсценируя сетевую атаку с использованием вредоносной программы — шифровальщика (иногда также называемой программой-вымогателем), преступники шифруют все данные, хранящиеся в компьютерной системе.

Помимо этого, для установления способа преступления и иных обстоятельств необходимо исследовать и изъять документы, регламентирующие в компании процессы в сферах информационной безопасности и информационных технологий: правила разграничения доступа, политику информационной безопасности, инструкции по организации парольной защиты и т. д.

Весьма важно, чтобы следователь осознавал, что из-за высокой волатильности информации в компьютерных системах обнаружение цифровых следов преступления при повторном либо дополнительном осмотре по прошествии времени в большинстве случаев будет маловероятным. В отсутствие гарантий того, что компьютерные системы, изъятие которых невозможно по тем или иным причинам, будут оставаться выключенными в течение разумных сроков, цифровые данные из них должны быть извлечены в избыточном количестве. Хотя такой подход увеличивает нагрузку на специалистов и экспертов вследствие большего объема данных, требующих исследования, его применение целесообразно, поскольку позволяет предотвратить потенциальную возможность утраты доказательств. Разумеется, при собирании избыточных цифровых данных необходимо руководствоваться принципом разумности, отбор информационных объектов производить, исходя из предпосылок, что в них может содержаться криминалистически значимая информация.

По окончании рабочего этапа осмотра места происшествия, оценки полноты и всесторонности его производства следователь составляет протокол, в котором, помимо прочего, подробно описывает действия специалиста, особенно если производилось исследование работающей компьютерной системы, сопровождающееся поиском и извлечением из нее цифровых следов, и примененное специалистом технико-криминалистическое и программное обеспечение. К протоколу прилагаются планы и схемы, например план размещения средств вычислительной техники в помещениях либо схема локальной сети, а также, при их наличии, результаты применения средств технической фиксации хода следственного действия, которые могут быть представлены в виде фото и видеозаписей, файла-журнала использованных специалистом в исследуемой компьютерной системе команд и результатов их исполнения, сохраненных на электронном носителе информации, и т. п.

К упаковке электронных объектов, изъятых при осмотре места происшествия (средств вычислительной техники, электронных носителей информации и др.), необходимо отнестись с особой тщательностью в связи с тем, что возможное физическое повреждение может привести к утрате хранящихся на них цифровых следов. Следует исключить иные риски для сохранности изымаемых данных, например разрушающее воздействие электромагнитного поля на определенные типы электронных носителей информации, такие как магнитные ленты. Современные средства вычислительной техники (смартфоны, планшеты, ноутбуки) используют различные технологии беспроводного об-

[20] *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. 4-е изд., перераб. и доп. М. : Норма, Инфра-М, 2013. С. 912.

мена данными по радиоканалам, предоставляя пользователю альтернативу для подключения к сети Интернет, например с помощью технологии Wi-Fi на основе стандартов IEEE 802.11 либо высокоскоростной передачи данных для мобильных телефонов, основанной на сетевых технологиях GSM/EDGE и UMTS/HSPA. При изъятии мобильных устройств с заблокированным экраном иногда бывает затруднительно определить, в каком состоянии они находятся — выключенном или энергосберегающем. В иных случаях выключение устройства может быть признано нецелесообразным, но при этом отсутствует возможность отключить адаптеры беспроводной связи, тогда устройство необходимо поместить в специальную изолирующую упаковку, чтобы исключить несанкционированное беспроводное подключение к нему посторонних лиц по протоколам удаленного управления и администрирования, в результате чего могут быть уничтожены или фальсифицированы цифровые следы.

Тактические особенности производства обыска сходны с особенностями осмотра места происшествия, но имеют свою специфику. Кажущееся очевидным решение об изъятии без предварительного исследования обнаруженных в ходе обысков компьютеров, мобильных устройств либо электронных носителей информации при определенных обстоятельствах приводит к утрате сведений, имеющих доказательственное значение, поскольку современные ноутбуки, планшеты, мобильные смартфоны и др. снабжены средствами защиты пользовательской информации, интегрированными производителями в свои продукты на программном или аппаратном уровне. Помимо этого, преступники принимают меры к сокрытию следов преступления, устанавливая на используемое ими компьютерное оборудование программы для шифрования и уничтожения данных.

Одним из эффективных способов избежать утраты значимых для расследования сведений является осмотр работающих средств вычислительной техники, когда доступ к сохраненной на них информации не ограничен. В этом случае специалисту необходимо либо скопировать данные, относящиеся к делу, на отдельный накопитель информации, либо обеспечить возможность повторного включения компьютерной техники без утраты хранящейся информации. Однако само наличие такой возможности зависит от подготовленности к производству обыска, наличия детально разработанного плана следственного действия, предусматривающего возможные проблемные ситуации, прогнозирование таких ситуаций и рассмотрение вариантов их решений, а также от грамотной реализации разработанного плана.

Учитывая многообразие способов уничтожения либо шифрования данных, хранящихся в компьютерных системах и иных средствах вычислительной техники, а также изобретательность лиц, совершающих компьютерные преступления, что обусловлено их высоким образовательным уровнем, склонностью к нестандартному мышлению и творческим подходом к осуществляемой ими деятельности, трудно переоценить этап подготовки к проведению обыска.

В отличие от осмотра места происшествия, обыск производится только по возбужденному уголовному делу, проведение обыска по горячим следам по делам о компьютерных преступлениях — скорее исключение из правил, в связи с чем у следователя имеется возможность подготовиться должным образом к такому сложному следственному действию. Как и в случае с осмотром места происшествия, необходимо заранее подобрать специалиста, обладающего необходимыми компетенциями, и совместно с ним разработать план обыска. Для составления плана следует предварительно собрать максимально полную информацию о месте производства обыска и находящемся там компьютерном оборудовании, о личности подозреваемого, используемых им средствах вычислительной техники, образе его жизни, графике бодрствования и сна, времени, которое он проводит за компьютером, и т. д. Значимую информацию можно получить путем проведения оперативно-розыскных мероприятий; из показаний лиц из окружения подозреваемого, сотрудничающих со следствием; посредством изучения статистических данных сетевых подключений, предоставленных провайдером, оказывающим подозреваемому услуги доступа в сеть Интернет, и/или оператором сотовой связи. Проведение подготовительных мероприятий позволяет исключить ошибки, связанные с неправильным установлением места проведения обыска (например, когда квартира была установлена по выделенному для ее владельца IP-адресу, а преступная деятельность осуществляется из соседнего помещения вследствие компрометации беспроводной точки доступа), а также минимизировать вредные

последствия от несвоевременности производства обыска, когда подозреваемый отдыхает, средства вычислительной техники выключены, а вся хранящаяся в них информация надежно зашифрована.

При проведении обыска в офисе, где преступную деятельность осуществляет группа лиц, следует выяснить планировку помещений, расположение рабочих мест, средств вычислительной техники, вспомогательного оборудования, необходимость привлечения дополнительно специалистов. После изучения собранной информации следователю надлежит убедиться в наличии специальных технико-криминалистических средств и программного обеспечения для предварительного исследования компьютерных устройств и цифровых следов, с учетом возможного оказания подозреваемым противодействия, иного оборудования для поиска, обнаружения, копирования и фиксации компьютерной информации, в том числе электронных носителей для хранения на них цифровых следов либо изготовления побитовых копий дисков, а также кабелей, переходников, набора инструментов для разборки технического оборудования, упаковочного материала.

При проведении обыска по делам о компьютерных преступлениях крайне важно обеспечить своевременность и внезапность проникновения следственной группы в обыскиваемое помещение, что обусловлено той легкостью, с которой подозреваемый может уничтожить цифровые следы, имеющие криминалистическое значение. Главная задача на этом этапе — получить доступ к средствам вычислительной техники, находящимся во включенном состоянии, с подключенными внешними носителями информации. Затем, не сбавляя темпа, необходимо отстранить подозреваемого и иных лиц, находящихся в помещении, от компьютеров, силовых кабелей, электрических розеток и исключить их несанкционированное передвижение по помещению. Грамотное использование следователем фактора внезапности, который, как правило, влечет кратковременное психопатологическое состояние растерянности у подозреваемого, может помочь склонить последнего к сотрудничеству со следствием. В этом случае следует получить от подозреваемого и зафиксировать в протоколе реквизиты доступа к локальным учетным записям и аккаунтам на внешних ресурсах, пароли для разблокирования мобильных устройств, данные для доступа к шифрованным дискам и т. п.

Вместе с тем, независимо от готовности подозреваемого сотрудничать со следствием, специалисту следует незамедлительно после проникновения в помещение начать работу по осмотру и предварительному исследованию средств вычислительной техники. В первую очередь необходимо, используя различные способы, исключить переход в режим энергосбережения или блокировки работающих компьютеров и мобильных устройств (например, путем периодического перемещения компьютерной мыши). Одновременно посредством фотосъемки либо видеозаписи следует запечатлеть содержимое экранов компьютеров, тем самым зафиксировать факт использования средств вычислительной техники в преступных целях на случай внезапного выключения питания и утраты возможностей для поиска цифровых следов преступления.

Крайне важная для расследования информация — машинный код, данные о сетевых подключениях, активных процессах, вычисленных хеш-функциях паролей, введенных пользователем как для локальных целей, например для подключения зашифрованной области диска, так и для авторизации на удаленных ресурсах, и т. п. — хранится в энергозависимой оперативной памяти компьютера. Сведения, которые могут быть получены в результате исследования содержимого оперативной памяти, иными способами зачастую добыть невозможно, однако при этом они характеризуются высокой волатильностью и уничтожаются при выключении питания. Для последующего поиска цифровых следов преступления в содержимом оперативного запоминающего устройства (ОЗУ) следует создать его копию с помощью специальной криминалистической программы, сохраненной на отдельном внешнем электронном носителе информации. Содержимое ОЗУ копируется в работающей системе путем подключения к ней электронного носителя со специальной программой. Извлеченные таким образом цифровые следы сохраняются на этом же либо ином внешнем диске, который изымается и приобщается к протоколу следственного действия.

Исходя из конкретных обстоятельств дела и с учетом ранее собранных на этапе подготовки к обыску сведений о возможных средствах и методах, которые могут быть применены обыскиваемым для уничтожения цифровых следов преступления, перед копированием содержимого ОЗУ целесообразно произвести осмотр информации, обрабатываемой компьютерной

системой. Например, для противодействия следствию подозреваемый может настроить запуск программы уничтожения данных либо просто выключение компьютера на событие операционной системы — изменение аппаратного окружения. В этом случае при подключении внешнего электронного носителя к программе для снятия копии содержимого ОЗУ будет выполнено запрограммированное действие.

Для выявления признаков, свидетельствующих о наличии в системе криминалистически значимых сведений, которые могут быть утрачены в результате противодействия подозреваемого, следует:

— провести поиск на предмет обнаружения программ, обеспечивающих шифрование файлов; программ для создания и использования шифруемых областей цифровых данных (криптоконтейнеров); программ, обеспечивающих функционирование виртуальных машин; программ — менеджеров паролей; программ — клиентов мгновенного обмена сообщениями, поддерживающих шифрование трафика; программ для написания приложений — среды разработки; специфических утилит (программ-спамеров и т. п.);
— изучить файловую систему с целью исследования логической структуры дисков на предмет выявления неразмеченной области большого размера и обнаружения файлов больших размеров, возможно являющихся криптоконтейнерами;
— исследовать запущенные на компьютере процессы, изучить аппаратное и сетевое окружение, проверить на наличие подключений к удаленным сетевым ресурсам, в том числе облачным хранилищам, и т. п.

Информация, выводимая на монитор в ходе предварительного исследования компьютерной системы, должна быть зафиксирована посредством фотосъемки либо видеозаписи. В отсутствие уверенности, что после выключения средств вычислительной техники данные на них не будут зашифрованы либо доступ к ним не будет ограничен иными способами, необходимо скопировать все значимые для расследования данные на специально приготовленный электронный носитель информации. Такими сведениями могут быть архив электронной почты; контактные листы программ-клиентов обмена сообщениями; история переписки; исходные коды; среда разработки и скомпилированные образцы программного обеспечения; данные о доступе к серверам, веб-ресурсам и другой сетевой инфраструктуре; файлы, содержащие копии веб-страниц, посещенных с помощью браузеров; файлы, содержащие историю посещения веб-страниц; настройки VPN; профили пользователей; отсканированные изображения финансовых и регистрационных документов и т. п.

Кроме этого, обязательно следует скопировать файлы из доступных криптоконтейнеров в локальной системе, а при наличии активных подключений к сетевым ресурсам, в том числе облачным хранилищам, произвести удаленное копирование данных на внешний носитель информации, который приобщить к протоколу обыска.

Если непосредственное подключение через интерфейс USB носителя информации к осматриваемой системе невозможно, в том числе из соображений обеспечения сохранности цифровых следов, следует рассмотреть иные способы для извлечения и сохранения криминалистически значимой информации, например посредством копирования данных на сетевой диск с использованием протокола SMB.

При изъятии выключенной компьютерной системы, когда изучить ее конфигурацию, аппаратное окружение и подключенные диски не представляется возможным, обыскиваемое помещение необходимо тщательно осмотреть и, при необходимости, исследовать с помощью специальной аппаратуры с целью проверки, не использует ли подозреваемый удаленные сетевые диски, которые физически могут быть скрыты в стенах, нишах мебельных гарнитуров, подсобных помещениях.

Действия специалиста, направленные на осмотр и предварительное исследование средств вычислительной техники, извлечение и сохранение на внешний носитель цифровых данных, а также иные манипуляции, совершенные с целью поиска цифровых следов преступления, должны быть детально описаны в протоколе обыска, по возможности запечатлены с помощью фотосъемки либо видеозаписи или зарегистрированы иными средствами фиксации хода и результатов следственного действия. Использованные в ходе обыска специальные технические и программные средства должны быть указаны в протоколе. Подлежат фиксации в протоколе обыска также действия подозреваемого, направленные на противодействие следственной группе, например попытки уни-

чтожить цифровые данные, обесточить средства вычислительной техники, заблокировать мобильное устройство.

Все компьютерные устройства, накопители информации и другие предметы, изъятые согласно протоколу обыска, должны быть соответствующим образом упакованы, чтобы исключить риски уничтожения либо повреждения цифровых следов и предотвратить несанкционированное удаленное подключение к ним с использованием сети Интернет, о возможностях которого было упомянуто выше.

Выемка средств вычислительной техники и электронных носителей информации требует несколько меньше организационных усилий. В большинстве случаев допущенные при ее проведении ошибки технического характера не являются существенными. Тем не менее подготовительные мероприятия необходимы и заключаются в привлечении к производству следственного действия компетентного специалиста в соответствии с требованиями ч. 2 ст. 164.1 УПК РФ. Заметим, что участие специалиста в производстве выемки не должно носить формальный характер. При выемке средств вычислительной техники специалист может проверить их работоспособность, уточнить особенности функционирования, оказать содействие следователю в составлении протокола при описании технических аспектов.

Журнальные файлы доступа к ресурсам и копии содержимого серверов либо облачных хранилищ информации предоставляются провайдерами соответствующих услуг на электронных носителях информации, изъятие которых целесообразно производить в рамках выемки. Также в рамках выемки изымаются имеющие криминалистическое значение результаты внутреннего расследования, проведенного службой информационной безопасности пострадавшей организации. При выемке электронных носителей информации, содержащих криминалистически значимую информацию, следует убедиться в ее наличии, доступности на изымаемом диске и отразить тип и признаки изымаемой информации в протоколе.

Изъятые в ходе осмотра места происшествия, обыска или выемки средства вычислительной техники и электронные носители информации, а равно содержащиеся на них цифровые следы нуждаются в последующем исследовании. Предварительное исследование, предшествующее назначению судебной экспертизы, возможно провести в рамках осмотра предметов с привлечением специалиста, с использованием многофункциональных возможностей универсальных криминалистических комплексов с высоким уровнем автоматизации, например комплексов Belkasoft Evidence или «Мобильный криминалист». Интерфейс таких систем оптимизирован для работы пользователей без углубленных специальных знаний, в связи с чем их применение часто называют исследованием с помощью одной кнопки — PBF (от англ. push-button forensics). Вместе с тем существует риск утраты цифровых следов, поскольку такие комплексы не в состоянии обработать нестандартную ситуацию[21].

При осмотре средств вычислительной техники и накопителей информации важно следовать общим правилам по работе с цифровыми данными. Для обеспечения неизменности информации подключение электронных носителей, в том числе копий дисков, следует производить исключительно с использованием специальных устройств-блокираторов. Включение осматриваемого компьютерного устройства допускается в исключительных случаях, когда иным образом извлечь криминалистически значимую информацию невозможно. В этом случае все манипуляции с устройством и цифровыми следами должны быть детально отражены в протоколе осмотра предмета и, по возможности, зафиксированы посредством фотосъемки либо видеозаписи или зарегистрированы иным техническим способом.

Отдельно в ряду невербальных следственных действий при расследовании компьютерных преступлений стоит следственный эксперимент. Его целью в большинстве случаев является установление возможностей использования определенных информационно-коммуникационных технологий, средств вычислительной техники, программного обеспечения, сетевых ресурсов и сервисов для осуществления данного способа преступления, деталей механизма преступного события. Например, в процессе эксперимента может быть установлен факт взаимодействия вредоносной программы-бота с сервером управления, подтверждающий версию следствия, что проверяемые части программного обеспечения являются единым

[21] *James J. I.*, *Gladyshev P.* Challenges with Automation in Digital Forensic Investigations // URL: https://arxiv.org/pdf/1303.4498 (дата обращения: 11.07.2021).

программным комплексом, разработанным с применением сетевой архитектуры «клиент-сервер». В другом случае с помощью следственного эксперимента может быть установлена фальсификация представленной в свою защиту подозреваемым электронной переписки, которая якобы была сохранена в результате резервного копирования в облачном хранилище данных.

К проведению эксперимента с использованием информационно-коммуникационных технологий, как и в случае с другими невербальными следственными действиями, в рамках которых подразумевается работа с цифровыми следами, в обязательном порядке следует привлекать специалиста. Опытные действия с применением компьютерных устройств могут осуществляться как специалистом, так и непосредственно лицом, действия которого проверяются. Если проверяются действия, производимые подозреваемым, предпочтительно, чтобы он лично демонстрировал их участникам следственного действия. Недопустимо, чтобы в опытных мероприятиях использовались изъятые по делу средства вычислительной техники и носители информации, так как это приведет к модификации хранящихся на них цифровых следов. Для этих целей следует использовать аналогичное оборудование, возможности которого достаточны для проверки соответствующих фактов. Помимо детального документирования проводимого опытного мероприятия, в протоколе следственного действия, ход и результаты эксперимента могут быть зафиксированы посредством фотосъемки и видеозаписи, с помощью журналирования действий в компьютерной системе, сохранения результатов эксперимента в файл, записи экрана и т. п.

Если в ходе следственного эксперимента получены новые данные, представленные в виде цифровых следов, они должны быть сохранены специалистом на приготовленном для этих целей электронном носителе информации. Идентифицирующие признаки полученных данных (хеш-сумма, размер и т. п.) следует внести в протокол, а электронный носитель приобщить к протоколу следственного эксперимента.

БИБЛИОГРАФИЯ

1. *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. — 4-е изд., перераб. и доп. — М. : Норма, Инфра-М, 2013. — 928 с.
2. *Белкин Р. С.* Курс криминалистики. — 3-е изд., доп. — М. : Юнити-Дана, Закон и право, 2001. — 837 с.
3. *Вехов В. Б.* Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. — 2016. — № 4 (11). — С. 46–50.
4. *Россинская Е. Р.* Криминалистика : учебник для вузов. — М. : Норма, 2016. — 464 с.
5. *Россинская Е. Р.* Направления инновационного развития криминалистической тактики и методик расследования в условиях глобальной цифровизации // II Минские криминалистические чтения : материалы Международной научно-практической конференции (Минск, 10 декабря 2020 г.) : в 2 ч. — Минск : Академия МВД Республики Беларусь, 2020. — Ч. 1. — С. 207–211.
6. *Россинская Е. Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. — 2019. — № 2 (99). — С. 193–202.
7. *Россинская Е. Р.*, *Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы Международной научно-практической конференции (19 февраля 2019 г.). — Алматы : Алматинская академия МВД Республики Казахстан, 2019. — С. 6–9.
8. *Россинская Е. Р.*, *Семикаленова А. И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. — 2020. — Т. 11. — Вып. 3 : Право. — С. 745–759.
9. *Россинский С. Б.* Следственные действия : монография. — М. : Норма, 2018. — 240 с.
10. *Рядовский И. А.* Компетенции специалиста по работе с цифровыми следами при производстве следственных действий // Законы России. Опыт. Анализ. Практика. — 2020. — № 9. — С. 94–100.
11. *Чекунов И. Г.*, *Голованов С. Ю.* [и др.] Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учеб. пособие. — 2-е изд. / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2019. — 198 с.

12. *Casey E.* Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. — Academic Press, 2011. — 840 p.
13. Introduction to Cybercrime. United Nations Office on Drugs and Crime // URL: https://www.unodc.org/e4j/en/tertiary/cybercrime.html (дата обращения: 11.07.2021).
14. *James J. I.*, *Gladyshev P.* Challenges with Automation in Digital Forensic Investigations // URL: https://arxiv.org/pdf/1303.4498 (дата обращения: 11.07.2021).
15. *Maras M.-H.* Cybercriminology. — Oxford University Press, 2016. — 448 p.
16. McGuire and Dowling. Cybercrime: A review of the evidence. Research Report 75. Chapter 2 : Cyber-enabled crimes-fraud and theft // URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf (дата обращения: 11.07.2021).

Материал поступил в редакцию 21 июля 2021 г.

REFERENCES

1. Averyanova TV, Belkin RS, Korukhov YuG, Rossinskaya ER. Kriminalistika: uchebnik dlya vuzov [Criminalistics: A textbook for universities]. 4th ed., rev. and suppl. Moscow: Norma: Infra-M; 2013. (In Russ.)
2. Belkin RS. Kurs kriminalistiki [The course in criminology]. 3rd ed., suppl. Moscow: Unity-Dana: Zakon i pravo; 2001. (In Russ.)
3. Vekhov VB. Elektronnye dokazatelstva: problemy teorii i praktiki [Electronic evidence: Problems of theory and practice]. *Pravoporyadok: istoriya, teoriya, praktika [Legal Order: History, Theory, Practice]*. 2016;4(11):46-50. (In Russ.)
4. Rossinskaya ER. Kriminalistika: uchebnik dlya vuzov [Criminalistics: A textbook for universities]. Moscow: Norma-Infra-M; 2016. (In Russ.)
5. Rossinskaya ER. Napravleniya innovatsionnogo razvitiya kriminalisticheskoy taktiki i metodik rassledovaniya v usloviyakh globalnoy tsifrovizatsii [Directions of innovative development of forensic tactics and investigative techniques in the context of global digitalization]. In: *II Minskie kriminalisticheskie chteniya: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii (Minsk, 10 dekabrya 2020 g.): v 2 ch. [2nd Minsk forensic readings: Proceedings of the International Scientific and Practical Conference (Minsk, December 10, 2020). In 2 parts]*. Minsk: Academy of the Ministry of Internal Affairs of the Republic of Belarus; 2020. Part 1. P. 207-211. (In Russ.)
6. Rossinskaya ER. Teoriya informatsionno-kompyuternogo obespecheniya kriminalisticheskoy deyatelnosti: kontseptsiya, sistema, osnovnye zakonomernosti [Theory of information and computer support of criminalistic activity: concept, system, main regularities]. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii*. 2019;2(89):193-202. (In Russ.)
7. Rossinskaya ER, Ryadovskiy IA. Kontseptsiya tsifrovykh sledov v kriminalistike [The concept of digital traces in criminology]. In: *Aubakirovskie chteniya: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii (19 fevralya 2019 g.) [Aubakirov Readings: Proceedings of the International Scientific and Practical Conference (February 19, 2019)]*. Almaty: Almatinskaya akademiya MVD Respubliki Kazakhstan; 2019. (In Russ.)
8. Rossinskaya ER, Semikalenova AI. Osnovy ucheniya o kriminalisticheskom issledovanii kompyuternykh sredstv i sistem kak chast teorii informatsionno-kompyuternogo obespecheniya kriminalisticheskoy deyatelnosti [Fundamentals of the doctrine of forensic research of computer tools and systems as part of the theory of information and computer support for forensic activities]. *Vestnik Sankt-Peterburgskogo universiteta. Pravo [Vestnik of Saint Petersburg University. Law].* 2020;11(3):745-759. (In Russ.)
9. Rossinskiy SB. Sledstvennye deystviya: monografiya [Investigative actions: A monograph]. Moscow: Norma; 2018. (In Russ.)
10. Ryadovskiy IA. Kompetentsii spetsialista po rabote s tsifrovymi sledami pri proizvodstve sledstvennykh deystviy [The competence of a specialist in working with digital traces in the production of investigative actions*]. Zakony Rossii. Opyt. Analiz. Praktika [The laws of Russia. Experience. Analysis. Practice].* 2020;9:94-100. (In Russ.)
11. Chekunov IG, Golovanov SYu, et al. Metodicheskie rekomendatsii po rassledovaniyu prestupleniy v sfere kompyuternoy informatsii: ucheb. posobie [Methodological recommendations for the investigation of crimes

in the field of computer information. A textbook]. 2nd ed. Moscow: Moskovskiy universitet MVD Rossii imeni V. Ya. Kikotya Publishing house; 2019. (In Russ.)
12. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press; 2011. (In Eng.)
13. Introduction to Cybercrime. United Nations Office on Drugs and Crime. Available from: https://www.unodc.org/e4j/en/tertiary/cybercrime.html [cited 2021 July 11]. (In Eng.)
14. James JI, Gladyshev P. Challenges with Automation in Digital Forensic Investigations. Available from: https://arxiv.org/pdf/1303.4498 [cited 2021 July 11]. (In Eng.)
15. Maras M-H. Cybercriminology. Oxford University Press; 2016. (In Eng.)
16. McGuire and Dowling. Cybercrime: A review of the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes-fraud and theft. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf [cited 2021 July 11]. (In Eng.)