УДК 343.13
doi: 10.18323/2220-7457-2022-3-25-33

Следственные действия и типичные ошибки при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации

Сергеев Андрей Борисович, доктор юридических наук, профессор,
профессор кафедры уголовного процесса и экспертной деятельности
Челябинский государственный университет, Челябинск (Россия)

E-mail: Sergeev_ab@bk.ru

Аннотация: Телекоммуникационные технологии сделали возможным использование обществом виртуального, а не только реального (материального) пространства. Отдельные действия, наносящие вред общественным отношениям, попали под запрет уголовного законодательства: ст. 272, 273, 274, 274.1 УК РФ. Если расследуемые преступления, совершенные в материальном мире, имеют большую наработанную следственную и судебную практику, то расследование преступлений, совершенных в сфере компьютерной информации, имеет слабую эмпирическую базу и небольшой объем наработок научного характера. Это указывает на наличие криминалистически важной проблемы и необходимость ее решения. Содержание статьи составляет перечень и краткий криминалистический обзор допускаемых следственными органами типичных ошибок при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации. На основе системно-комплексного подхода представлен обзор криминалистически значимых для расследования элементов информационных компьютерных сетей, проведен анализ реализации положений доказательственного права при расследовании преступлений в телекоммуникационном пространстве. В заключение излагается суждение об универсальной природе цифрового следа. Называются типичные ошибки при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации. Отмечается, что такое положение ставит перед учеными и практиками задачу совершенствовать криминалистические методы, средства и тактику обнаружения следов преступления в информационном (виртуальном) пространстве и процессуального их закрепления в законодательно установленном порядке. В статье предлагается направление решения данной проблемы. Оно не указывает на необходимость переработки существующей теории доказательственного права и дополнения ее новыми процессуальными аспектами, фиксирующими особые качества цифровой информации. Подчеркивается, что допускаемые следователями ошибки не вызваны пробелами научного знания криминалистического или законодательного характера. Решение проблемы лежит в практической плоскости повышения уровня знаний IT-технологий следователями, осуществляющими расследование.

Ключевые слова: цифровое пространство; компьютерные сети; технологии; информация.

Для цитирования: Сергеев А.Б. Следственные действия и типичные ошибки при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2022. № 3. С. 25–33. DOI: 10.18323/2220-7457-2022-3-25-33.

ВВЕДЕНИЕ

Процесс установления истины об обстоятельствах совершенного преступления (ст. 73 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ)) нормативно определяется рядом алгоритмически последовательных этапов: собиранием, проверкой и оценкой доказательств (ст. 86–88 УПК РФ). Каждый из названных этапов также структурирован. Так, процесс собирания сведений формируется посредством совершения ряда криминалистически значимых действий: обнаружения сведений; их исследования на предмет установления отношения к устанавливаемому обстоятельству; фиксации этих относимых к устанавливаемому событию сведений в процессуально заданной форме [1; 2].

Как этап процесса доказывания, собирание доказательств состоит в производстве следственных действий (ч. 1 ст. 86 УПК РФ) с детальным отражением порядка их производства, процессуального закрепления их результатов (фиксация и изъятие). Собирание доказательств субъект доказывания может осуществлять и посредством производства иных (помимо следственных) процессуальных действий, которые процессуальным законодательством определены как требования, запросы, поручения (ч. 4 ст. 21 УПК РФ).

Устанавливая признаки вещественного доказательства, УПК РФ не перечисляет виды их проявления. Исключение сделано в отношении цифровой информации. Вещественные доказательства – источники, содержащие цифровую информацию, в ряде норм определяемые конкретным термином «электронные носители информации». Для названного вида доказательств процесс доказывания (собирание, проверка и оценка доказательств) имеет правовые особенности. В настоящее время нельзя считать, что все они выявлены и учитываются следственными подразделениями при производстве по уголовным делам. Научные исследования по уяснению феномена «электронные доказательства» и результаты этих исследований доказывают, что важно сблизить позиции ученых и практиков по понятию (содержанию) категории «виртуальный след» [3; 4]. Единообразное понимание специалистами понятия этой категории существенно усилит эффективность

следственной и судебной деятельности. Итоговые судебные решения по уголовным делам не будут вызывать сомнений в своей правосудности [5; 6].

В настоящее время существующий разброс мнений относительно влияния развития цифровых технологий на уголовное судопроизводство можно свести к трем основным позициям (в рамках каждой позиции суждения можно дополнительно конкретизировать).

Первая позиция характеризуется радикальными положениями. Она гласит, что цифровизация влечет за собой формирование информационно-коммуникационной модели, которая делает необходимой реорганизацию всего уголовно-процессуального механизма судопроизводства. Парадигма уголовно-процессуального доказывания должна быть кардинально перестроена. Это относится и к предмету доказывания, и к средствам доказывания, и к субъектам производства по уголовному делу.

Согласно этой позиции, высокий уровень развития цифровых технологий уже сейчас позволяет отказаться от существующей системы следственных действий, как объективно устаревшей. Взамен «наследия прошлого» нужно разработать «универсальное» следственное действие [7].

Доказательствами должны стать любые носители, стандарты допустимости доказательств следует пересмотреть. Достоверность доказательств (сведений) может обеспечивать не вызывающая разумных сомнений цепь «законных владений» цифровой информацией. Цифровизация в уголовном судопроизводстве делает избыточной функцию «предварительного следствия» (всестороннего полного и объективного раскрытия и расследования преступления). Программист, специалист по информационной безопасности корпорации, «робот», любой «пользователь» цифровой технологией может успешно обеспечить сбор необходимых сведений [8].

Вторая, «умеренная» позиция. Предлагается, не меняя существующей уголовно-процессуальной концепции построения уголовного судопроизводства, закрепить в уголовном судопроизводстве фактическое положение об использовании цифровых технологий, законодательно раскрыть категорию «цифровая информация», закрепить понятие «носитель цифровой информации» [9]. В стадии возбуждения уголовного дела порядок (последовательность) производства процессуальных действий по обнаружению признаков преступления, а также результат этих действия предлагается фиксировать одним из двух способов: на материальном носителе (например, протокол осмотра) или в цифровой форме (в электронном виде). Разрабатываются предложения электронного предупреждения о юридической ответственности, регламентация процессуального порядка идентификации и аутентификации [10; 11]. Цифровизация должна привести к уточнению отдельных существующих следственных действий. «Контроль и запись переговоров» (ст. 186 УПК РФ) предлагается переименовать в «контроль электросвязи»; «контроль телефонных и иных переговоров» заменить на «контроль электросвязи» [12].

Третья позиция, согласно которой следует придерживаться традиционной исторически сложившейся концепции российского уголовного судопроизводства. Утверждается, что цифровизация не меняет концептуальных основ уголовного судопроизводства, но ставит вопрос обнаружения и фиксации информации, расположенной в виртуальном пространстве. Этот вопрос большей частью имеет технический характер. Для отправления правосудия предлагаемая «уголовно-процессуальная революция» вредна. «Революция» не заменит классический уголовный процесс каким-то «новым» уголовным процессом [13].

В подтверждение обоснованности такого подхода приводятся соответствующие аргументы. Так, утверждается, что «электронный протокол» от своего бумажного аналога уголовно-процессуальной сущностью отличаться не может, содержание будет всегда едино – сведения об обстоятельствах совершения расследуемого преступления. Отличие только в техническом исполнении протокола. Признание электронной информации отдельным источником уголовно-процессуальных доказательств породит многочисленные коллизии в устоявшейся правовой доктрине уголовного процесса [12].

Реализация предложений специалистов, разделяющих первую (радикальную) позицию о цифровизации уголовного судопроизводства, невозможна. При таком «инновационном» подходе экспертные возможности оказания помощи следствию будут ничтожно малы. Так, перевод вещественных доказательств в формат 3D-версии исключит возможность проведения экспертных исследований по оставленным на материальном носителе физическим и генетическим следам.

Еще более актуализируется проблема сохранения достоверности материалов электронного уголовного дела. Если материалы дела будут находиться в электронных сетях, риск несанкционированного допуска и изменения содержания материалов дела существенно возрастет.

Из трех приведенных точек зрения автор придерживается третьей позиции. В работе предпринята попытка аргументированно доказать перспективность развития именно традиционного исторически сложившегося направления законодательной регламентации уголовного судопроизводства.

Гипотеза исследования – допускаемые типичные ошибки при обнаружении и изъятии следователями доказательств преступных действий в сфере компьютерной информации вызваны не издержками существующей теории доказательственного права; проблема лежит в практической плоскости и связана с недостаточным уровнем знаний информационно-телекоммуникационных технологий (IT-технологий) следователями, осуществляющими расследование.

Цель работы – рассмотрение проблемных вопросов выявления особенностей следов преступления в цифровой системе, специфики процессуальной деятельности по их закреплению, анализ типичных ошибок при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации.

МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ

Этапы исследования:

– уточнение перечня элементов тех информационных компьютерных технологий, которые могут быть носителями криминалистически значимой для расследования информации о преступных действиях виновных лиц;

– систематизация доказательственного права, нормы которого могут применены при расследовании преступлений в виртуальной среде;

– выявление резервов криминалистической тактики при подготовке и производстве следственных действий по обнаружению и процессуальному закреплению цифровой информации в компьютерной сети;

– анализ типичных ошибок следственных органов при работе с цифровым следом.

Материалами настоящего исследования послужили: 1) положения федерального законодательства; 2) материалы судебной практики; 3) обобщенные результаты ранее проведенных исследований по рассматриваемым вопросам.

Методологическими средствами исследования явились:

– догматический метод – использование понятий правовых конструкций, устоявшихся в юриспруденции, имеющих четкую формальную определенность и ясность (норма права, доказательства как сведения об устанавливаемых событиях и пр.);

– системный метод в виде системно-структурного, системно-функционального, системно-целевого аналитико-правового исследования для выявления многообразных типов связей в цифровом информационном пространстве. Знание о типах связей помогает воссоздать картину преступных действий и закрепить виртуальную информацию о них в классическую уголовно-процессуальную форму.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Особенности следовой картины преступных действий в телекоммуникационной сфере

Механизм преступных действия в сфере компьютерной информации (ст. 272–274.4 УК РФ) представляет собой комплекс действий лица по подготовке к совершению неправомерного доступа. Комплекс складывается из способа неправомерного доступа, примененного при совершении преступления в информационной системе (он обуславливает специфику электронного следа при уничтожении, блокировании, модификации компьютерной информации), а также действий по сокрытию следов преступления [14].

Особенность криминалистически значимых сведений об обстоятельствах преступления заключается в том, что сведения могут содержаться как в одном, так и в нескольких электронных носителях, если они объединены в одну информационную систему. Информационную систему же формирует база информации (данных). Электронная база данных создается и обновляется за счет разнообразных специализированных IT-технологий, представляющих собой набор средств и методов применения этих технологий с целью обнаружения, обработки, передачи и накопления в них сведений (информационного продукта)[1]. Электронная база данных хранится в памяти компьютера[2].

Совокупность электронных баз данных в судебной практике[3] часто определяют через понятие «виртуальное пространство». Возможность синхронизации и последовательной реализации столь разнообразной деятельности по созданию баз данных (виртуального пространства) формирует структуру электронной комплексной системы.

Требования к качественному досудебному производству складываются из необходимости обеспечения полноты, всесторонности расследования [15].

Полнота предварительного расследования обеспечивается максимально полным обнаружением следов преступления. В сфере цифрового общения следы преступной деятельности распределяются в структурных частях электронной системы. Представленные выше сведения об информационной комплексной системе и входящих в нее подсистемах нужны следователю для того, чтобы в практической поисковой процессуальной деятельности он мог быстро восстанавливать в сознании весь перечень процессуально значимых источников, в которых могут находиться в цифровой форме сведения об обстоятельствах преступной деятельности (ст. 73 УПК РФ).

Чтобы осуществлять эффективное собирание, проверку и оценку доказательств преступления, совершенного в сфере компьютерной информации, следователь должен знать следующие основные положения о материальных электронных объектах, обеспечивающих возможность развития общественных отношений, в том числе криминальных, в цифровом информационном пространстве:

а) информационное пространство образуют информационные компьютерные сети;

б) информационные компьютерные сети формируются структурными элементами. Из них базовыми являются:

– компьютеры (иные сетевые узлы);

– сетевое оборудование ;

– информационное и программное обеспечение.

При совершении преступных действий их следы «оседают» в каждой из названных подсистем;

в) идентификация лица осуществляется не с помощью методов и правил габитоскопии. В компьютерной вычислительной сети установление пользователя осуществляется посредством определения электронной подписи, паролей, установлением кода доступа, учетных записей, цифрового имени пользователя.

Установление обстоятельств, подлежащих доказыванию по уголовному делу (ст. 73 УПК РФ), во многом определяется компонентным составом компьютерной сети и их взаимообусловленным функционированием. Базовый элемент компьютерной сети (такой как подсистема), структурные составляющие которого могут быть источниками доказательственной информации

[1] *Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».*

[2] *Ч. 2 статьи 1260 Гражданского кодекса Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ в ред. от 11.06.2021 // Консультант-Плюс: справочно-правовая система.*

[3] *Постановление Суда по интеллектуальным правам от 20.06.2019 № С01-390/2019 по делу № А40-169068/2018; Постановление Арбитражного суда Московского округа от 29.11.2019 № Ф05-18806/2019 по делу № А40-217942/2018 Требование: О взыскании неосновательного обогащения // Консультант-Плюс: справочно-правовая система.*

об обстоятельствах совершенного преступления, представляет собой объединенные в группы компьютеры и ряд других компьютерных устройств (специалисты называют их телекоммуникационными сетевыми узлами), связанных друг с другом каналом связи и реализующих соответствующую программу.

Другим базовым элементом компьютерной сети является информационное программное обеспечение. В состав программного обеспечения включены программы для ЭВМ. Программа – составленная разработчиком в цифровом виде система команд и необходимых данных, обеспечивающих работу ЭВМ и связанных с ЭВМ иных устройств. Понятием «программа ЭВМ» охватываются также комбинации компьютерных инструкций и данных, позволяющих аппаратному обеспечению вычислительной системы выполнять вычисления или функции управления. Аналогичное направление построений имеют и криминальные программы, целевая направленность которых определяется решением задач уничтожения, блокировки, изменения, модификации, осуществления несанкционированного владельцем копирования компьютерной информации, нейтрализации средств охраны компьютерной информации и пр.

Источники цифровой информации с самой информацией, в них содержащейся, признаются относимыми к расследуемому преступлению, если они были использованы в качестве орудия преступления или они являлись оборудованием, которое использовалось для совершения преступного деяния; восприняли воздействие преступного посягательства и хранят на себе следы этого воздействия; стали предметом преступного посягательства (ч. 1 ст. 81 УПК РФ). Процессуальным качеством относимости цифровая информация с носителем будет обладать в случае, если ее можно использовать в процессе обнаружения иных доказательств совершенного преступления и лиц, его совершивших [16].

Следует согласиться со специалистами в том, что появление цифровой следовой картины делает востребованным и актуальным активизацию исследований и разработку (адаптирование) криминалистических методов поиска и фиксирования следов преступлений, предусмотренных ст. 272, 273, 274, 274.1 УК РФ [17; 18].

Цифровая информация в компьютерной сети распространяется по заданным программами маршрутам «в виде последовательной и полной цепи отраженных … сведений, замкнутых по смыслу» [19, с. 31]. Существо содержания криминалистически значимого следа заключается (проявляется) в изменениях цифровой информации [20], в разнице между тем «как было» до преступного воздействия и «как стало» после завершения «атаки».

Таким образом, чтобы получить сведения об обстоятельствах расследуемого преступления в сфере компьютерной информации, субъект расследования при проведении следственных действий должен обладать навыками специалиста в сфере обмена цифровой информацией:

– исследовать хранящуюся в компьютерной цепи цифровую информацию;

– обнаруживать среди этой информации сведения, подтверждающие совершенное преступление (найти электронный след);

– фиксировать результаты поисковой деятельности в процессуальных документах.

Порядок производства следственных действий не зависит от вида доказательства и складывается из трех этапов: подготовительного, рабочего и заключительного.

Практическими работниками часто недооценивается подготовительный этап к проведению следственного действия по обнаружению и закреплению цифровой информации [21].

Ряд исследователей пытается распространить существующую теорию доказательств на электронные доказательства [22; 23]. Указывается, что специфика природы электронных доказательств не требует разработки дополнительных теорий доказательственного права. Существующие положения криминалистической тактики применимы и к цифровым следам [24]. Например, одна из задач следственного действия по обнаружению следов преступления заключается в тщательном подборе участников следственного действия; другая – в принятии решения о необходимом криминалистическом оборудовании для обнаружения и изъятия доказательственной цифровой информации [25]. Сказанное относится и к специалисту, и к понятым, которым были бы ясны действия следователя и специалиста на протяжении всего процесса проведения следственного действия.

Следователь должен правильно определить типологию сети. Ошибка может привести к существенным потерям информации.

Уголовно-процессуальное законодательство не устанавливает обязательного участия специалиста при производстве обыска (ст. 182 УПК РФ) и выемки (ст. 183 УПК РФ), однако целесообразность его присутствия в ряде сложных следственных ситуаций очевидна и объективно необходима. Востребованность участия специалиста вызвана обладанием им знаниями в области цифровой коммуникации участников общественных отношений. На этапе подготовки к производству следственного действия в порядке, предусмотренном ст. 58, 164, 168 УПК РФ, специалист может помочь следователю определиться с выбором необходимого комплекта криминалистической техники по обнаружению, фиксации и изъятию цифровой информации.

Экспертно-криминалистические подразделения комплектуются в основном программно-аппаратными комплексами «Мобильный Криминалист Эксперт».

Исследования показывают, что при расследовании преступлений в сфере компьютерной информации подготовительный этап включает производство промежуточных следственных действий, результаты которых создают благоприятные условия для производства планируемого следственного действия. Так, при подготовке к производству обыска (выемке) и получению значимой доказательственной цифровой информации в организации с большой и разветвленной компьютерной сетью, следователи предварительно проводят допрос системного администратора информационной системы. В силу его компетенции и обязанности системный администратор может сообщить важные для успешного производства обыска (выемки) сведения, которыми он располагает в силу своего положения. Такими могут быть сведения:

– о типологии (структуре) информационной локальной системы, с одного из сетевых узлов которой осуществлена атака;

– о входящих в информационную сеть объектах, их состоянии, технических возможностях; информирование о типовой характеристике, наименовании, комплектующих особенностях, идентифицирующих объект. Сюда же относятся сведения о маркировочных знаках, номера серии и пр.;

– о схемах нахождения сетевых узлов и их взаимного расположения друг относительно друга, последовательности соединения и пр.

– о работоспособности сети;

– о местах концентрации криминалистически значимой информации: на сервере или на отдельных компьютерах сотрудников и пр.;

– о специфике работы web-сервера;

– об операционной системе и пр.

При выполнении действий по обнаружению и изъятию доказательственной информации в ряде случаев используют помощь специалиста уже на подготовительном этапе. На этом этапе специалист может оказать помощь в ответе на вопрос о наличии (отсутствии) угрозы противодействия проведению следственного действия и уничтожения цифровой информации и ее носителей. При реальности такой угрозы следователь предусматривает и принимает меры к исключению возможности ее возникновения за счет использования фактора внезапности производства следственного действия, привлечения сил и средств блокирования доступа к сети, дистанционного на нее воздействия с целью размагничивания носителей и таким способом уничтожения цифровой следовой картины. Ч. 7 ст. 164 УПК РФ закрепляет право следователя использовать сотрудников оперативных подразделений при производстве следственного действия.

Рабочий этап следственного действия

Рабочий этап следственного действия (обыск, выемка) направлен на обнаружение и изъятие носителей цифровой информации, доказывающих совершение преступлений, предусмотренных ст. 272, 273, 274, 274.1 УК РФ.

При производстве следственного действия следователь получает от специалиста:

– рекомендации по тактике производства следственного действия;

– рекомендации по поиску и изъятию доказательственной информации, правильному копированию сведений;

– консультацию при определении средств, обеспечивающих шифрование информации (сведений), ее фиксацию и места хранения;

– помощь при выявлении средств, предназначенных для того, чтобы в неординарной ситуации уничтожить информацию, и нейтрализации этих средств;

– помощь в описании изымаемых объектов;

– помощь в фиксировании доказательственной информации с удаленных сетевых ресурсов, идентификации данных и пр.

– помощь следователю при составлении протокола [26].

С учетом общих требований (ст. 164, 164.1, 166 УПК РФ) строгое соблюдение нормативных положений ст. 182, 183 УПК РФ обеспечивает допустимость доказательств. Отсутствие в протоколе следственного действия максимально подробного описания порядка и последовательности его проведения ставит под сомнение достоверность полученных результатов. Наиболее часто повторяющимися ошибками являются следующие пробелы в описании информационной (компьютерной) сети и узлов, которые подвергнуты обыску: не указан вид информационной вычислительной сети (персональная или локальная); отсутствуют сведения, является ли сеть закрытой (доступ к ней имеет только ограниченный круг лиц, имеющий отношение к этому предприятию) или открытой (кроме пользователей учреждения, доступ к сети имеют иные лица); какие операционные системы установлены (Windows, UNIX, NetWare, Cisco IOS).

Полученные результаты суд признает недопустимыми, если не указаны криминалистические средства и порядок их применения при обнаружении и изъятии электронных носителей с доказательственной информацией (ч. 3 ст. 164.1 УПК РФ) [27].

К протоколу должны прилагаться видеозапись (если она применялась) и схемы расположения сетевых узлов. Если в сети была обнаружена цифровая информация (сведения), то приложением к протоколу будут электронные носители, содержащие эти доказательственные сведения (карты памяти, флеш-накопители и т. п.) (ч. 8 ст. 166 УПК РФ).

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Установленный перечень особенностей следов преступления в цифровой системе, специфика деятельности по процессуальному закреплению этих следов, анализ типичных ошибок при обнаружении и изъятии доказательств преступных действий в сфере компьютерной информации подтверждают гипотезу об ошибочности предложений по радикальной реорганизации всего уголовно-процессуального механизма судопроизводства и смены парадигмы уголовно-процессуального доказывания. Не нашли подтверждения необходимости и предложения частичной корректировки ряда норм УПК РФ в связи с образованием цифрового следа от преступной деятельности и необходимостью закрепления этого следа. Традиционная исторически сложившаяся концепция российского уголовного судопроизводства показывает свою эффективность в современных условиях и поэтому должна быть сохранена.

Представленный краткий системно-комплексный обзор научных положений, суждений, представлений о цифровом пространстве у специалистов в области уголовного судопроизводства в целом:

– дает представление о состоянии научных познаний об этой специфичной области цифрового пространства;

– позволяет определить векторную направленность научных исследований и установить перспективные направления;

– организовать исследование сложных вопросов расследования, которые до настоящего времени исследуются недостаточно активно, но ответы на которые востребованы практикой. Такое отставание – результат до конца не осознанного потенциала важности решения этих вопросов для качества уголовного судопроизводства.

Представленное в работе обобщение типичных ошибок следственных органов при производстве по уголовным делам и использовании в качестве доказательств по делу цифровой информации при всей своей значимости не является исчерпывающим. Современное знание о следственных ошибках не является полным. Требуется дальнейшее обобщение следственной и судебной практики, выявление сложностей работы с цифровой доказательственной базой.

Следует согласиться с научной общественностью, что определяющим эффективность производства по уголовному делу фактором являются глубокие познания субъекта расследования (следователя, дознавателя) в различных видах и сочетаниях компьютерных сетей, компьютерных устройств, компьютерных технологий. В зависимости от сочетания названных особенностей информационных комплексов, перспективным направлением криминалистической науки следует признать дальнейшее развитие теории формирования следственных ситуаций [28] при расследовании преступлений в цифровом пространстве.

ВЫВОДЫ

Изложенное позволяет заключить следующее:

1. Практика расследования преступлений в сфере компьютерной информации достаточно убедительно свидетельствует об отсутствии потребности перерабатывать и дополнять существующую теорию доказательственного права новыми процессуальными аспектами, фиксирующими особые качества цифровой информации.

2. В то же время универсальная природа цифрового следа очевидна. Такое положение ставит перед учеными и практиками задачи совершенствования криминалистических методов, средств и тактики обнаружения следов преступления в информационном (виртуальном) пространстве и процессуального закрепления этих следов в законодательно установленном порядке.

3. В процессе обнаружения и фиксации следов преступления в сфере компьютерной информации допускаемые следователями ошибки не вызваны пробелами научного знания криминалистического или законодательного характера. Проблема лежит в практической плоскости и связана с недостаточным уровнем знаний IT-технологий следователями, осуществляющими расследование.

Решение этой проблемы лежит в направлениях:

– большей специализации субъектов доказывания преступной деятельности в рассматриваемой сфере общественной (цифровой) деятельности;

– вопреки мнению ряда специалистов, в сохранении требования закона об обязательном участии специалиста в производстве обыска и выемке (ч. 2 ст. 164.1 УПК РФ).

СПИСОК ЛИТЕРАТУРЫ

1. Вехов В.Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. 2016. № 1. С. 155–158. EDN: VUGRPP.
2. Россинский С.Б. Собирание, формирование и исследование доказательств в уголовном судопроизводстве: проблемы разграничения // Российская юстиция. 2017. № 5. С. 24–27. EDN: YNDPYZ.
3. Поляков М.П., Смолин А.Ю. Концептологический анализ феномена электронных доказательств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 2. С. 135–145. DOI: 10.24411/2078-5356-2019-10222.
4. Голубцов В.Г. Электронные доказательства в контексте электронного правосудия // Вестник гражданского процесса. 2019. Т. 9. № 1. С. 170–188. EDN: YZYAYX.
5. Россинский С.Б. Дискуссионные вопросы методологии уголовно-процессуального познания // Российская юстиция. 2016. № 4. С. 32–36. EDN: VSAWUN.
6. Глухова Е.В., Сергеев А.Б. Вопросы имплементации европейского правового стандарта проведения ОРМ по доказыванию в виновности лица в совершении преступления в российское уголовно-процессуальное законодательство // Евразийский юридический журнал. 2017. № 3. С. 220–225. EDN: YJUHXB.
7. Александров А.С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 130–139. EDN: XWCHZB.
8. Доктринальная модель уголовно-процессуального доказательственного права Российской Федерации и комментарии к ней / под ред. А.С. Александрова. М.: Юрлитинформ, 2015. 299 с.
9. Зазулин А.И. Компьютерная информация в уголовном процессе: сущность и способы закрепления в качестве доказательств по уголовному делу // Проблемы экономики и юридической практики. 2015. № 6. С. 130–133. EDN: VGSKGN.
10. Балашова А.А. Место и роль электронных носителей информации в системе источников доказательств // Образование. Наука. Научные кадры. 2018. № 4. С. 76–79. EDN: VOHAFC.
11. Масленникова Л.Н., Топилина Т.А. Зарубежный опыт использования онлайн-сервисов для подачи сообщения о преступлении // Законность. 2020. № 6. С. 61–65. EDN: CDXJDI.
12. Черкасов В.С. Компьютерная информация как самостоятельный источник уголовно-процессуальных доказательств: аргументы за и против // Вестник Дальневосточного юридического института МВД России. 2018. № 2. С. 55–62. EDN: USGVSW.
13. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25. DOI: 10.24411/2414-3995-2019-10002.
14. Мира К.А. Возможности использования криминалистических цифровых платформ при расследовании преступления // Эксперт-криминалист. 2021. № 2. С. 32–34. EDN: VEKKBI.
15. Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199–207. DOI: 10.17223/15617793/448/25.
16. Сергеев А.Б., Сергеев М.А., Сергеев К.А. Особенности расследования преступлений, связанных с присвоением прав на владение и управление предпри-

ятиями и организациями. Челябинск: ГОУ ВПО ЧЮИ МВД России, 2008. 127 с.
17. Зайцев О.А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 4. С. 42–57. DOI: 10.12737/jflcl.2019.4.4.
18. Кальницкий В.В. Вопросы правовой регламентации следственных действий на современном этапе // Законы России: опыт, анализ, практика. 2015. № 2. С. 32–38. EDN: TOMORX.
19. Колычева А.Н. Криминалистические аспекты работы следователя при изъятии электронно-цифровых следов в компьютерной системе и сети Интернет // Юридическое образование и наука. 2017. № 4. С. 30–33. DOI: 10.18572/2072-4438-2017-4-30-33.
20. Гаврилин Ю.В., Балашова А.А. Процессуальный порядок собирания доказательств на энергонезависимых локальных электронных носителях информации // Сибирский юридический вестник. 2020. № 2. С. 77–82. EDN: LLSSCT.
21. Большаков М.С. Основные ошибки осмотра места происшествия и пути их преодоления следователями органов внутренних дел // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2020. № 1. С. 12–14. EDN: XQRLPN.
22. Количенко А.А. Доктринальный подход к определению термина «электронные доказательства» в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 3. С. 136–140. DOI: 10.36511/2078-5356-2021-3-136-140.
23. Шигуров А.В., Шигурова Е.И. Проблемы правовой регламентации использования электронных следов и электронных носителей информации при производстве по уголовному делу // Гуманитарные и политико-правовые исследования. 2020. № 1. С. 53–63. EDN: EBIAKZ.
24. Бердникова О.П. Порядок получения электронных доказательств при проведении отдельных следственных действий // Право и государство: теория и практика. 2022. № 1. С. 366–368. DOI: 10.47643/1815-1337_2022_1_366.
25. Перов В.А. Электронные следы при расследовании уголовных дел о преступлениях с использованием криптовалют // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4. С. 108–111. EDN: OJSDEF.
26. Аносов А.В. Предупреждение соучастия несовершеннолетних в преступлениях в цифровую эпоху // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 2. С. 14–19. DOI: 10.37973/KUI.2022.60.84.002.
27. Соркин В.С., Козел В.М. Об электронных доказательствах в уголовном процессе (проблемы правоприменения) // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2021. Т. 11. № 2. С. 79–84. EDN: XLAMXN.
28. Шубарина Л.В., Сергеев А.Б. Учение Л.Я. Драпкина о следственных ситуациях в условиях цифровизации предварительного расследования // Вклад Л.Я. Драпкина в криминалистическую науку. Екатеринбург: Уральский государственный юридический университет, 2019. С. 364–374. EDN: ZMQGDC.

REFERENCES

1. Vekhov V.B. The concept, types and features of fixing electronic evidence. *Rassledovanie prestupleniy: problemy i puti ikh resheniya*, 2016, no. 1, pp. 155–158. EDN: VUGRPP.
2. Rossinskiy S.B. The gathering, formation and study of evidence in criminal proceedings: problems of differentiation. *Rossiyskaya yustitsiya*, 2017, no. 5, pp. 24–27. EDN: YNDPYZ.
3. Polyakov M.P., Smolin A.Yu. Concept-centred analysis of the phenomenon electronic evidence. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii*, 2019, no. 2, pp. 135–145. DOI: 10.24411/2078-5356-2019-10222.
4. Golubtsov V.G. Electronic evidence in the context of e-justice. *Vestnik grazhdanskogo protsessa*, 2019, vol. 9, no. 1, pp. 170–188. EDN: YZYAYX.
5. Rossinskiy S.B. Discussion methodological issues of criminal procedural knowledge. *Rossiyskaya yustitsiya*, 2016, no. 4, pp. 32–36. EDN: VSAWUN.
6. Glukhova E.V., Sergeev A.B. The European legal standard of conduct search and investigation for proving the guilt of the perpetrator of the crime in comparison with the Russian criminal-procedural legislation. *Evraziyskiy yuridicheskiy zhurnal*, 2017, no. 3, pp. 220–225. EDN: YJUHXB.
7. Aleksandrov A.S. The problems of the theory of criminal procedural proof, which must be solved in connection with the transition to the digital age. *Sudebnaya vlast i ugolovnyy protsess*, 2018, no. 2, pp. 130–139. EDN: XWCHZB.
8. Aleksandrov A.S., ed. *Doktrinalnaya model ugolovno-protsessualnogo dokazatelstvennogo prava Rossiyskoy Federatsii i kommentarii k ney* [Doctrinal model of criminal procedural evidentiary law of the Russian Federation and commentary to it]. Moscow, Yurlitinform Publ., 2015. 299 p.
9. Zazulin A.I. Computer information in criminal procedure: essense and methods of fixing as an evidence in criminal case. *Problemy ekonomiki i yuridicheskoy praktiki*, 2015, no. 6, pp. 130–133. EDN: VGSKGN.
10. Balashova A.A. The place and role of electronic media in the system of sources of evidence. *Obrazovanie. Nauka. Nauchnye kadry*, 2018, no. 4, pp. 76–79. EDN: VOHAFC.
11. Maslennikova L.N., Topilina T.A. International experience of use of online services for submission of a crime report. *Zakonnost*, 2020, no. 6, pp. 61–65. EDN: CDXJDI.
12. Cherkasov V.S. Computer information as an independent source of criminal procedure evidence: arguments for and against. *Vestnik Dalnevostochnogo yuridicheskogo instituta MVD Rossii*, 2018, no. 2, pp. 55–62. EDN: USGVSW.

13. Golovko L.V. The digitalization in criminal procedure: local optimization or global revolution? *Vestnik ekonomicheskoy bezopasnosti*, 2019, no. 1, pp. 15–25. DOI: 10.24411/2414-3995-2019-10002.
14. Mira K.A. Opportunities for the use of criminalistic digital platforms in crime investigation. *Ekspert-kriminalist*, 2021, no. 2, pp. 32–34. EDN: VEKKBI.
15. Aleksandrov A.S., Andreeva O.I., Zaytsev O.A. On development prospects of the Russian criminal proceeding in the context of digitalization. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2019, no. 448, pp. 199–207. DOI: 10.17223/15617793/448/25.
16. Sergeev A.B., Sergeev M.A., Sergeev K.A. *Osobennosti rassledovaniya prestupleniy, svyazannykh s prisvoeniem prav na vladenie i upravlenie predpriyatiyami i organizatsiyami* [Features of the investigation of crimes related to the assignment of rights to possession and management of enterprises and organizations]. Chelyabinsk, GOU VPO ChYuI MVD Rossii Publ., 2008. 127 p.
17. Zaytsev O.A. Features of the use of electronic information as criminal evidence: a comparative-legal analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatelstva i sravnitelnogo pravovedeniya*, 2019, no. 4, pp. 42–57. DOI: 10.12737/jflcl.2019.4.4.
18. Kalnitskiy V.V. Academy of the Russian interior ministry, honored lawyer of the Russian Federation. *Zakony Rossii: opyt, analiz, praktika*, 2015, no. 2, pp. 32–38. EDN: TOMORX.
19. Kolycheva A.N. Criminalistical aspects of the investigator's work at withdrawal of digital traces in a computer system and the internet network. *Yuridicheskoe obrazovanie i nauka*, 2017, no. 4, pp. 30–33. DOI: 10.18572/2072-4438-2017-4-30-33.
20. Gavrilin Yu.V., Balashova A.A. Procedural procedure for collecting evidence on non-volatile local electronic media. *Sibirskiy yuridicheskiy vestnik*, 2020, no. 2, pp. 77–82. EDN: LLSSCT.
21. Bolshakov M.S. Main errors of inspection of the place of accident and ways to overcome them by investigators of internal affairs bodies. *Prestupnost v sfere informatsionno-telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy*, 2020, no. 1, pp. 12–14. EDN: XQRLPN.
22. Kolichenko A.A. Doctrinal approach to the definition of the term "electronic evidence" in criminal proceedings. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii*, 2021, no. 3, pp. 136–140. DOI: 10.36511/2078-5356-2021-3-136-140.
23. Shigurov A.V., Shigurova E.I. Problems of legal regulation of the use of electronic tracks and electronic media in the criminal proceedings. *Gumanitarnye i politiko-pravovye issledovaniya*, 2020, no. 1, pp. 53–63. EDN: EBIAKZ.
24. Berdnikova O.P. The procedure for obtaining electronic evidence during individual investigative actions. *Pravo i gosudarstvo: teoriya i praktika*, 2022, no. 1, pp. 366–368. DOI: 10.47643/1815-1337_2022_1_366.
25. Perov V.A. Electronic traces in the investigation of criminal cases of crimes involving the use of cryptocurrency. *Vestnik Akademii Sledstvennogo komiteta Rossiyskoy Federatsii*, 2020, no. 4, pp. 108–111. EDN: OJSDEF.
26. Anosov A.V. Prevention of minor complicity in crimes in the digital age. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*, 2022, vol. 13, no. 2, pp. 14–19. DOI: 10.37973/KUI.2022.60.84.002.
27. Sorkin V.S., Kozel V.M. On electronic evidencein criminal proceedings (problems of law enforcement). *Vestnik Grodnenskogo gosudarstvennogo universiteta imeni Yanki Kupaly. Seriya 4. Pravovedenie*, 2021, vol. 11, no. 2, pp. 79–84. EDN: XLAMXN.
28. Shubarina L.V., Sergeev A.B. Uchenie L.Ya. Introduction of digital technologies in the preliminary investigation and the doctrine of L.Ya. Drapkin on investigative situations. *Vklad L.Ya. Drapkina v kriminalisticheskuyu nauku*. Ekaterinburg, Uralskiy gosudarstvennyy yuridicheskiy universitet Publ., 2019, pp. 364–374. EDN: ZMQGDC.

Crime investigations and common mistakes when detecting and withdrawing the evidence of cyber criminal actions

Andrey B. Sergeev, Doctor of Sciences (Law), Professor,
professor of Chair of Criminal Procedure and Expert Activity
Chelyabinsk State University, Chelyabinsk (Russia)

E-mail: Sergeev_ab@bk.ru

Abstract: Telecommunication technologies made it possible for the society to use both real (material) and virtual space. Some actions injuring social relations fall under the criminal legislation prohibition: Articles 272, 273, 274, and 274.1 of the RF Criminal Code. The investigated crimes committed in the material world have a large tried and tested investigative and judicial practice, but the investigation of cyber crimes has a weak empirical base and a limited scientific experience. This indicates the existence of a criminalistically significant problem and the necessity of its solution. The paper presents the list and brief criminalistic overview of common mistakes made by investigative authorities when detecting and withdrawing the evidence of cyber crimes. Based on the system-comprehensive approach, the author gives an overview of information computer network elements criminalistically significant for an investigation; carries out the analysis of the implementation of evidentiary law provisions when investigating crimes in the telecommunication space. In conclusion, the author explains the digital footprint universal nature and enumerates typical mistakes when detecting and withdrawing the evidence of cyber criminal acts. The paper states that such order of things sets before the scientists and practitioners the task of improving forensic methods, tools, and tactics for detecting traces of a crime in the information (virtual) space and their procedural legal enshrinement. The author proposes a direction of solving this problem. It does not indicate

the necessity to revise the existing evidentiary law theory and to supplement it with new procedural aspects fixing special characteristics of digital information. The author highlights that the mistakes made by investigators are not caused by the gaps in scientific knowledge of a forensic or legislative nature. The problem solution lies in the practical plane of the IT-technologies knowledge improvement by the investigators conducting the examination.

Keywords: digital space; computer networks; technologies; information.

For citation: Sergeev A.B. Crime investigations and common mistakes when detecting and withdrawing the evidence of cyber criminal actions. *Vektor nauki Tolyattinskogo gosudarstvennogo universiteta. Seriya: Yuridicheskie nauki*, 2022, no. 3, pp. 25–33. DOI: 10.18323/2220-7457-2022-3-25-33.