УДК 343.9+340.6
ББК 67.5
С56

С56 Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: материалы научно-практической конференции с международным участием (г. Москва, 5 апреля 2019 г.). – Москва : РГ-Пресс, 2019. — 248 с.

ISBN 978-5-9988-0919-4
DOI 10.31085/9785998809194-2019-248

5 апреля 2019 года в Московском государственном юридическом университете имени О.Е. Кутафина (МГЮА) состоялась научно-практическая конференция с международным участием «Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности». Инициаторами и организаторами конференции выступили кафедра судебных экспертиз и кафедра криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА).

В сборник вошли представленные участниками научно-практической конференции с международным участием материалы, в которых освещаются проблемы защиты прав и законных интересов граждан и юридических лиц в условиях цифровизации на основе специальных знаний в области криминалистического исследования компьютерных средств и систем, в области речеведческих, экономических, почерковедческих, портретных, медицинских экспертиз, рассматриваются инструменты защиты от недостоверных экспертных данных в эпоху высоких технологий, иные проблемы, возникающие при назначении и производстве судебных экспертиз.

Тезисы выступлений и статьи печатаются в авторской редакции в алфавитном порядке по фамилиям авторов. Мнение автора не всегда совпадает с точкой зрения редакции.

Для научных работников, студентов, аспирантов и преподавателей вузов, практикующих юристов, а также широкого круга читателей, проявляющих интерес к судебным экспертизам.

УДК 343.9+340.6
ББК 67.5

Конференция проводилась в соответствии с грантом РФФИ в рамках научного проекта № 18-29-16003/18 «Концепция информационно-компьютерного обеспечения криминалистической деятельности».

Сборник подготовлен с использованием СПС «КонсультантПлюс».

Научное издание

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ КРИМИНАЛИСТИЧЕСКОЙ И СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ
МАТЕРИАЛЫ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ С МЕЖДУНАРОДНЫМ УЧАСТИЕМ (Г. МОСКВА, 5 АПРЕЛЯ 2019 Г.)
Сборник тезисов

Подписано в печать 28.08.2019. Формат 60×90 $^{1}/_{16}$.
Печать цифровая. Печ. л. 15,5. Тираж 50 экз.

ISBN 978-5-9988-0919-4
DOI 10.31085/9785998809194-2019-248

ОГЛАВЛЕНИЕ

или о загрязнении образца ДНК одного человека ДНК другого. Но самое главное для баз данных это то, что для кодирования любого снипа согласно предложенного нами принципа оцифровки достаточно всего 4 бит (полбайта) информации, причем представленных сразу в двоичном коде уже в виде первичных данных, благодаря чему объем хранимой информации в базах данных по каждому человеку с учетом реперной информации не превысит одного килобайта.

Таким образом, ДНК-идентификация личности с помощью высокополиморфных однонуклеотидных замен обеспечит максимальный уровень цифровизации, поскольку базы данных по этим элементам генома будут высокоструктурированными и будут иметь фиксированные границы в виде определенного числа ячеек, измениться которое не может ни при каких обстоятельствах, а хранимый объем даст необходимую информацию при минимальном занимаемом пространстве компьютерной памяти.

Данная работа выполнена в рамках гранта РФФИ-мк № 18-29-14076 по теме «Правовые и этические аспекты всеобщей ДНК-паспортизации населения Российской Федерации для целей ДНК-идентификации личности».

Антонов О. Ю.,

д. ю. н., доцент,
Московская академия Следственного комитета Российской Федерации,
декан факультета магистерской подготовки юридического института

Взаимодействие с интернет-провайдером в целях собирания цифровых следов

Анализ статистических данных, сформированных ГИАЦ МВД России на базе отчета о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, № 1-ВТ по форме № 615, утвержденного Приказом МВД России от 1 апреля 2002 г. № 311, за 2012-2018 годы[1], свидетельствует о том, что в 2015–2018 годах, в сравнении с 2012–2014 годами, произошел резкий скачок регистрации таких преступлений – всего в 17 раз. Естественно, что правоохранительные органы были не готовы к такому валу преступности. Поэтому, несмотря на увеличение в два-три раза количества расследованных преступлений, число нераскрытых возросло

[1] По данным Информационно-статистического управления ГСУ СК России.

более кардинально – почти в 27 раз, что привело к снижению их раскрываемости[1] с 74,8% в 2012 до 26,6% в 2018:

Показатель	2012	2013	2014	2015	2016	2017	2018
зарегистрировано	10227	11104	10968	43816	65949	90587	174674
расследовано	6909	7648	5519	13444	15313	20424	43362
приостановлено	2330	3084	4438	25579	49111	63473	119742

Представленные статистические сведения свидетельствуют о необходимости разработки дополнительных криминалистических рекомендаций по расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, в первую очередь в целях собирания цифровых следов. Среди специфических особенностей совершения рассматриваемых преступлений можно отметить интересную закономерность механизма следообразования, которую выявил С.В. Пропастин, определив ее как опосредованное двухуровневое взаимодействие конечного пользователя с глобальной информационно-телекоммуникационной сетью. На первом уровне присутствует следовой контакт конечного пользователя со своей компьютерной системой, на втором уровне – следовой контакт компьютерной системы конечного пользователя с компьютерной системой сети доступа (Интернет-провайдера)[2]. Развивая указанное мнение применительно к преступлениям, в ходе которых осуществляется общение преступника и потерпевшего по электронным каналам связи, можно выделить дополнительные уровни такого взаимодействия: два аналогичных уровня применительно к потерпевшему, а также следовой контакт подключения друг к другу компьютерных систем обоих конечных пользователей (преступника и потерпевшего) через компьютерную систему сети доступа. В связи с этим, при расследовании таких преступлений повышается объективная необходимость осуществления взаимодействия с операторами связи в целях установления таких следовых контактов (соединений) преступника и потерпевшего.

---

[1] Данный термин не используется в статистической отчетности, однако проведенные в соответствии с порядком его формирования вычисления наглядно демонстрируют сложившуюся негативную ситуацию в борьбе с данным видом преступлений.

[2] См.: *Пропастин С. В.* Опосредованное двухуровневое взаимодействие как закономерность механизма преступлений, совершаемых с использованием интернет-технологий // Актуальные проблемы уголовной и уголовно-процессуальной политики Российской Федерации: материалы международной научно-практической конференции / отв. ред. И. Г. Рагозина, Ю. В. Деришев. Омск: Ом. юрид. акад., 2017. С. 224.

Согласно федеральному законодательству оператором связи признается юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии[1]. Таким образом, в качестве субъектов взаимодействия при расследовании преступлений будут выступать указанные лица, предоставляющие доступ в Интернет как преступнику, так и потерпевшему. Рассмотрим формы взаимодействия следователя с провайдерами на основе изучения обвинительного заключения по уголовному делу по факту совершения действий сексуального характера в отношении малолетнего К. в ходе видеообщения с использованием программного обеспечения «Skype»[2].

Распространенной формой взаимодействия с операторами связи, предоставляющими своим абонентам доступ в Интернет, является направление запросов (в порядке ч. 4 ст. 21 УПК РФ, Федеральных законов «Об оперативно-розыскной деятельности», «О полиции», «О следственном комитете Российской Федерации»), ответы на которые признаются доказательствами в качестве иных документов.

Так, по изученному уголовному делу первоначально провайдеру, предоставляющему услуги по месту жительства потерпевшего, был направлен запрос о принадлежность IP-адреса, с которого осуществлялось Интернет-соединение с потерпевшим. В ответе были указаны данные второго провайдера, который использовал данный IP-адрес в другом регионе России. Последний в ответ на запрос сообщил, что на основании договора о межоператорском взаимодействии данный IP-адрес был предоставлен третьему провайдеру. Однако для уточнения выделенных (реальных) IP-адресов, которые использовались компьютером потерпевшего в период трех сеансов видеосвязи с преступником, именно в ходе которых были совершены преступные действия, первому провайдеру был направлен повторный запрос. Ответ на него позволил конкретизировать запрос третьему провайдеру, который сообщил данные о конкретном лице, которому были предоставлены Интернет-услуги, с адреса которого в указанное время было соединение с IP-адресами потерпевшего. Таким образом был установлен К., совершивший это преступление.

Такая практика взаимодействия сформировалась уже давно и используется, в основном, в рамках оперативно-розыскной деятельности или проверки сообщений о преступлении, поэтому можно отнести ее к непроцессуальным формам взаимодействия. После

---

[1] Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ, п. 12, ст. 2 // СПС «КонсультантПлюс».

[2] Обвинительное заключение по уголовному делу № 201500069/74-2015 следственного отдела по Центральному административному округу г. Тюмени СУ СК России по Тюменской области. По материалам Московской академии СК России.

возбуждения уголовного дела такое взаимодействие должно осуществляться в процессуальной форме – в порядке, предусмотренном ст. 186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Согласно устоявшейся точке зрения, данное следственное действие признается комплексным, включающем в себя три обязательных элемента: а) получение от оператора связи списка соединений (детализации); б) осмотр детализации; в) приобщение ее к материалам уголовного дела в качестве вещественного доказательства[1]. В рассматриваемом случае у следствия возникает задача установления данных абонента, осуществлявшего соединение с IP-адресом потерпевшего. Поскольку в п. 24.1 ст. 5 УПК РФ указано, что «получение информации о соединениях между абонентами и (или) абонентскими устройствами – это получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), **номерах абонентов, других данных, позволяющих идентифицировать абонентов** (выделено нами), а также сведений о номерах и месте расположения приемопередающих базовых станций», то решение указанной задачи необходимо осуществлять именно в рамках данного следственного действия.

Возвращаясь к указанной выше форме непроцессуального взаимодействия с третьим провайдером, его ответ на запрос в лучшем случае может являться доказательством в качестве иного документа, поэтому требует подкрепления другими, более процессуально значимыми источниками доказательств. В связи с этим, по рассматриваемому уголовному делу следователь произвел допрос в качестве свидетеля индивидуального предпринимателя Р., в сферу деятельности которого входит оказание интернет-услуг для граждан. На допросе последний показал, что месяц назад в его адрес поступал запрос, согласно которому были предоставлены три IP-адреса, у которых происходило соединение с одним из его клиентов. Далее, он ввел указанные адреса в билинговую систему[2], в результате чего было установлено, что в указанный в запросе период эти IP-адреса осуществляли соединение с внутренним IP-адресом его клиента. После чего он ввел установленный IP-адрес в хранилище учетных записей и установил, что этим человеком является Л., которому Р. устанавливал Интернет-соединение около пяти лет назад. Однако

---

[1] *Стельмах В. Ю.* Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография. Екатеринбург: Уральский юридический институт МВД России, 2014. С. 59.

[2] Более подробно см., напр., *Дерикьянц П. П.* Обзор архитектур современных биллинговых систем и перспективы их развития // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2007. № 27. С. 143–164.

следователю стало недостаточно данных показаний и на следующий день он произвел с участием провайдера Р. осмотр программного комплекса и трафик-инспектора его персонального компьютера, в ходе анализа которого установлено, что в интересующий следствие период времени пользователем предоставляемой им Интернет-сети, осуществлявшим соединения с IP-адресами потерпевшего К., является клиент Л.

Таким образом, следователь дополнительно произвел два следственных действия, подтверждающие результаты первоначального запроса, исполненного месяц назад. Представляется, что в этом случае более оптимальным является проведение допроса представителя провайдера с разъяснением порядка его работы, учета абонентов, наличия программного обеспечения, позволяющего отследить Интернет-соединения своего абонента с другими IP-адресами в определенное время. После чего можно незамедлительно провести следственный осмотр программного комплекса и трафик-инспектора персонального компьютера провайдера в целях установления конкретного абонента. В данном осмотре сотрудник организации Интернет-провайдера может выступать в качестве специалиста, поскольку обладает специальными знаниями в области компьютерной техники, что позволит реализовать требования части 2 статьи 164.1 УПК РФ в случае необходимости копирования осмотренной информации с цифровых носителей данной организации. Проведение такого следственного осмотра с участием представителя оператора связи позволяет нейтрализовать недостатки рабочего этапа следственного действия – получения информации о соединениях между абонентами и (или) абонентскими устройствами, отмеченные в литературе: предумышленное искажение исходных сведений, человеческий фактор (халатность или ошибки при обработке данных), технические неполадки оборудования, предоставление объемного массива информации[1].

Еще одной дополнительной задачей взаимодействия следователя с провайдером может быть сбор по трафику и Интернет-активности конкретного абонента характеризующей его информации, в том числе установление его личной страницы в социальной сети, которая может быть оформлена на вымышленное имя.

Так, по изученному уголовному делу следователем с участием провайдера Р. осмотрена личная страница пользователя социальной сети «Вконтакте» «И. К.» с Интернет-адресом «https://vk.com/***»,

---

[1] *Дерюгин Р. А.* Криминалистические и процессуальные вопросы производства следственного действия, предусмотренного статьей 186.1 Уголовно-процессуального кодекса Российской Федерации // Вопросы безопасности. 2016. № 5. С. 43–48. URL: http://e-notabene.ru/nb/article_20396.html.

в ходе которого установлены 8 фотографий с изображением обвиняемого Л., которые сохранили на компьютер, после чего произвели печать указанных фотографий на 8 листов формата А4. Данные фотографии впоследствии были использованы в ходе предъявления для опознания потерпевшему К. и его матери, наблюдавшей сеанс видеообщения обвиняемого Л. с ее сыном. Именно на основании результатов данного следственного действия по месту жительства Л. в тот же день был произведен обыск, а сам Л. задержан по подозрению в совершении указанного преступления в порядке, предусмотренном ст. ст. 91-92 УПК РФ.

Аналогичная задача может решаться и в случае, если компьютерно-техническая экспертиза изъятого у подозреваемого, обвиняемого компьютерного оборудования не может определить историю его посещения Интернет-ресурсов, поскольку последним было произведено полное удаление данной информации. Но для этого необходимо знать время сеанса, так как IP-адрес выделяется динамическим и в разные периоды времени он может быть назначен различным устройствам. Поэтому данное обстоятельство следует выяснять в ходе допроса самого подозреваемого, обвиняемого либо его близких, родственников, друзей или соседей. Копирование данной информации с цифровых носителей провайдера может решить и иные задачи в ходе анализа (биллинга) его Интернет-соединений.

Таким образом, рассмотренный пример следственной практики позволяет сформулировать следующие криминалистические рекомендации по взаимодействию следователя (дознавателя) с Интернет-провайдером:

В случае необходимости установления фактов электронного общения в ходе подготовки к осуществлению взаимодействия необходимо выяснить три обстоятельства: IP-адрес потерпевшего и подозреваемого, а также даты и точное время их сеансов связи. При необходимости доказывания Интернет-соединения преступника и потерпевшего в конкретное время в первоначальном запросе или ходатайстве о производстве следственного действия, касающегося получения информации о соединениях между абонентами и (или) абонентскими устройствами, провайдеру, предоставляющему услуги потерпевшему, надо точно указывать эти периоды времени в целях установления используемых потерпевшим IP-адресов.

В случае наличия в материалах проверки сообщения о преступлении ответа Интернет-провайдера на запрос, направленный в рамках проведения оперативно-розыскных мероприятий, необходимо провести допрос представителя данной организации с целью выяснения порядка функционирования биллинговой системы и определения ее абонентов, следственный осмотр ее компьютерного оборудования

для подтверждения информации, содержащейся в ответе на запрос, а при необходимости дальнейшего анализа биллинговой информации – осуществить ее копирование в ходе данного осмотра.

До начала проведения следственных действий с участием заподозренного лица можно через Интернет-провайдера собрать характеризующий его материал, в том числе путем установления его страницы в социальных сетях.

В случае полного удаления истории посещения Интернет-ресурсов с компьютера подозреваемого, обвиняемого данную информацию можно получить у провайдера при установлении времени их сеансов.

Бахтеев Д. В.,

к. ю. н.,
Уральский государственный юридический университет,
доцент кафедры криминалистики

Перспективы использования систем искусственного интеллекта в экспертно-криминалистической деятельности[1]

Современные компьютерные технологии уже радикально поменяли многие аспекты человеческой жизнедеятельности. Цифровизация экономики уже ликвидирует одни профессии и создает другие, в-третьих – происходят или готовятся произойти значительные изменения. Большинство действий, совершаемых в юридической деятельности, в том числе при производстве судебных экспертиз, сводятся к обработке неизвестной информации и преобразования вероятного знания в достоверное. Эффективность таких операция находится в прямой зависимости от количества знаний и опыта субъекта, вследствие чего зачастую в содержательно схожих ситуациях могут быть приняты значительно различающие решения. Автоматизация и компьютеризация некоторых операций может позволить разгрузить исполнителя, предоставить ему большую эвристическую свободу и самостоятельность без утраты общей эффективности его деятельности. Наиболее современной технологией, позволяющем произвести подобные улучшения являются системы искусственного интеллекта (ИИ).

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16001\18 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».