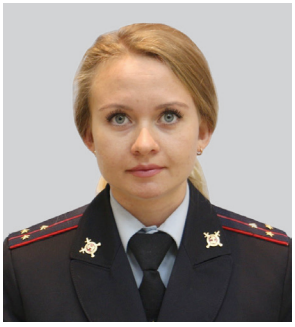
КРИМИНАЛИСТИЧЕСКИЕ ОСНОВЫ УСТАНОВЛЕНИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Александр Николаевич ПЕРШИН,
профессор кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доцент
pershin75@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9



Ксения Сергеевна СИДОРОВА,
адъюнкт адъюнктуры Омской академии МВД России
k_s159@mail.ru
644092, Россия, г. Омск, просп. Комарова, д. 7

Аннотация. *Одним из доказательств, подтверждающих или опровергающих виновность лица в совершении преступления, может являться оставленный им след. Вследствие совершения преступлений с использованием информационно-телекоммуникационных технологий заметно расширяется следовая картина — появляются новые, нетрадиционные следы. Современные информационные технологии позволяют решать задачи жизнедеятельности человека путем непосредственной эксплуатации сети самим пользователем либо генерирования необходимого результата цифровой технологией в автоматическом режиме по заранее разработанному алгоритму и предоставления его человеку. В результате этого в информационно-телекоммуникационной сети Интернет и устройствах доступа к ней образуется две группы следов. Первая группа следов является пользовательской информацией, преобразованной электронно-вычислительным устройством и представленной в семантически понятном для человека виде и свидетельствующей о самом человеке и (или) его деятельности. Ко второй группе следов относятся алгоритмизированные в виде буквенно-цифрового кода, т.е. порождаемые электронными вычислительными устройствами, программным обеспечением, функционированием информационных систем, используемые для приема, передачи, доставки, обработки и хранения электронных сообщений и документов.*

Ключевые слова: *след, информационно-телекоммуникационная сеть Интернет, пользователь, идентификатор, IP-адрес, доменное имя, никнейм, логин.*

DOI: 10.17803/2311-5998.2019.55.3.082-094

A. N. PERSHIN,
Professor of the Department of Criminalistics of the Kutafin Moscow State Law University (MSAL), Doctor of law, Docent
pershin75@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, 9

K. S. SIDOROVA,
the postgraduate student of the Omsk academy of the MIA
k_s159@mail.ru
644092, Russia, Omsk, prosp. Komarova, d. 7

CRIMINALISTIC BASES OF INSTALLING THE USER OF THE INFORMATION-TELECOMMUNICATION NETWORK INTERNET

Abstract. *One of the proofs confirming or disproving the guilt of a person in committing a crime may be the trace left by him. As a result of committing crimes with the use of information and telecommunication technologies, the following picture widens significantly — new, unconventional traces appear. Modern information technologies make it possible to solve problems of human life by direct exploitation of the network by the user, or by generating the necessary result by digital technology in an automatic mode using a previously developed algorithm and providing it to the person. As a result, two groups of traces are formed in the information and telecommunication network «Internet» and access devices to it. The first group of traces is user information, transformed by an electronic computing device and presented in a semantically understandable form for a person and indicating the person himself and / or his activity. The second group of traces includes algorithmized in the form of an alphanumeric code, i.e. generated by electronic computing devices, software, the functioning of information systems and are used to receive, transmit, deliver, process and store electronic messages and documents.*

Keywords: *trail, information and telecommunication network «Internet», user, identifier, IP-address, domain name, nickname, login.*

Исследования в области криминалистики показывают, что существует множество подходов к определению ее задач. Так, одна группа ученых полагает, что общей задачей криминалистики является содействие борьбе с преступностью своими специфическими силами и средствами, что обусловливает цель ее существования и развития[1]. Согласно позиции других ученых, общими задачами криминалистики являются обеспечение быстрого и полного

[1] См., например: *Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Россинская Е. Р.* Криминалистика : учебник для вузов / под ред. Р. С. Белкина. 2-е изд., перераб. и доп. М. : Норма, 2005. С. 51.

раскрытия и расследования преступлений, предотвращение и пресечение преступных посягательств[2].

Д. Н. Балашов, Н. М. Балашов, С. В. Маликов отмечают, что задачей науки криминалистики является разработка положений, рекомендаций правоохранительным и судебным органам для решения задач установления истины по уголовному делу[3].

В контексте заявленной темы статьи для нас более близка позиция тех авторов, которые считают, что общая задача криминалистики конкретизируется применительно к основным целевым назначениям уголовного судопроизводства, обозначенным действующим УПК РФ: обеспечение досудебного производства (предварительного следствия или дознания) по уголовному делу эффективными техническими средствами, приемами и методами его ведения; установление и изобличение лица или лиц, виновных в совершении преступления; создание необходимой доказательственной базы для их справедливого наказания или освобождения от него (ст. 6, 21 УПК РФ)[4].

Опираясь на изложенное, полагаем целесообразным отметить, что в основе решения задачи криминалистики, применительно к целевому назначению уголовного судопроизводства заложена поисково-познавательная деятельность соответствующих органов и должностных лиц, осуществляемая путем использования и совершенствования, существующих и создания новых средств и методов борьбы с преступностью.

Основополагающей задачей, стоящей перед органами расследования, является наиболее полное установление обстоятельств, подлежащих доказыванию, предусмотренных ст. 73 УПК РФ. Особый интерес представляет категория обстоятельств, устанавливающая виновность того или иного лица в совершении преступления, которая, по нашему мнению, является центральной и одновременно наиболее сложной для расследования, так как необходимы доказательства, подтверждающие или опровергающие виновность лица. Следует отметить, что одним из таких доказательств может являться след, образовавшийся в ходе преступления.

Криминалистическое учение о механизме следообразования подразделяет следы преступления по виду следа-носителя на материальные, когда в ходе совершения преступления происходят изменения в неживой природе, и идеальные, когда совершение преступления приводит к возникновению и закреплению мысленных образов в сознании и памяти людей. Соответственно, конечная цель исследования таких следов, как правило, будет состоять в установлении наличия или отсутствия непосредственной связи следа с физическим лицом.

В настоящее время информационно-телекоммуникационная сеть Интернет (далее — ИТС Интернет) предоставляет человеку широкие возможности по ее

---

[2] См., например: Криминалистика : учебник для экспертов-криминалистов / под ред. А. Г. Филиппова. М. : Юрлитинформ, 2005. С. 5.

[3] *Балашов Д. Н., Балашов Н. М.*, *Маликов С. В.* Криминалистика : учебник. 2-е изд. М. : Инфра-М, 2009. С. 3.

[4] См., например: Криминалистика : учебник / отв. ред. Н. П. Яблоков. 3-е изд., перераб. и доп. М. : Юристъ, 2005. С. 21.

использованию в силу своей общедоступности. Граждане активно пользуются различными услугами в сети Интернет, представленных на ее ресурсах: регистрируются на официальных сайтах с целью получения какой-либо государственной услуги, общаются на сайтах социальных сетей, совершают покупки в режиме онлайн на сайтах продаж. Причем такие действия могут быть обусловлены противоправными целями, связанными с совершением различных преступлений с использованием интернет-ресурсов.

В этой связи невозможно не согласиться с П. В. Мочагиным, который отмечает, что огромную роль в процессе совершения преступлений играет широкое распространение сети Интернет и ее ресурсов. Сегодня существует перечень деяний, которые наиболее распространены в сети. К ним относятся: интернет-мошенничества, нарушение права на неприкосновенность частной жизни, распространение порнографии, нарушение авторских и патентных прав, разглашение охраняемой законом государственной тайны, террористическая и экстремистская деятельность и т.д.[5]

Все вышеперечисленное позволяет говорить о том, что вследствие совершения преступлений с использованием информационно-телекоммуникационных технологий заметно расширяется следовая картина — появляются новые, нетрадиционные следы, которые могут быть использованы в целях раскрытия и расследования преступлений, доказывания виновности злоумышленников[6]. Таковыми могут быть «образные» следы, запечатлеваемые теле- и видеосистемами наблюдения, могущими фиксировать в том числе и звуковую среду совершения преступления, а также электронные, виртуальные следы, оставляемые кредитными, расчетными, социальными, дисконтными картами, устройствами мобильной связи, по которым можно четко отследить действия и передислокацию их обладателей, а в ряде случаев — выявить и пресечь противоправную смену их владельца[7].

Всякий выход пользователя в ИТС Интернет при помощи компьютера, смартфона, планшета и прочих цифровых устройств приводит к образованию следов его пребывания в сети. Но, как отмечает В. Б. Вехов, сведения, которые могут являться доказательствами по уголовному делу, могут быть зафиксированы на электронном носителе человеком с применением соответствующих технических устройств и автоматом — быть результатом работы алгоритма программы для электронных вычислительных машин[8]. Действия, обусловленные автоматической работой программы, берут свое начало из основ искусственного интеллекта, под которым понимаются компьютерные программы, программные комплексы, спо-

[5] *Мочагин П. В.* Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе // Вестник Удмуртского университета. Серия «Экономика и право». 2013. № 2. С. 148—154.

[6] *Ищенко Е. П.* Российская криминалистика сегодня // О криминалистике и не только : избранные труды. М. : Проспект, 2016. С. 38—46.

[7] *Ищенко Е. П.* Актуальные направления развития криминалистики // Актуальные вопросы криминалистики и уголовно-процессуального права : мат-лы конф. Киров, 2005. С. 7—11.

[8] *Вехов В. Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. 2016. № 1 (11). С. 155—158.

собные не просто действовать по заранее заданному алгоритму, но и реализовывать такие имманентные человеку творческие функции, как прогнозирование, оценка рисков, работа с неполными данными и т.д.[9]

Исходя из этого, следует заявить о том, что современные информационные технологии позволяют решать задачи жизнедеятельности человека путем непосредственной эксплуатации сети самим пользователем либо генерирования необходимого результата цифровой технологией в автоматическом режиме по заранее разработанному алгоритму и предоставления его человеку. В результате этого в ИТС Интернет и устройствах доступа к ней образуются две группы следов.

Первая группа следов является пользовательской информацией, преобразованной электронно-вычислительным устройством, представленной в семантически понятном для человека виде и свидетельствующей о самом человеке и (или) его деятельности. Такие следы могут быть информацией, распространение которой на территории Российской Федерации запрещено; сведениями, связанными с преступной деятельностью или информацией о лице, причастном к преступлению, выраженной в виде текстовых, табличных, графических, аудио- или видеоданных. Эта группа следов в связи с подготовкой, совершением или сокрытием преступления попадает в сферу внимания правоохранительных органов, как правило, в числе первых.

Ко второй группе следов мы относим алгоритмизированные в виде буквенно-цифрового кода, т.е. порождаемые электронными вычислительными устройствами, программным обеспечением, функционированием информационных систем, используемые для приема, передачи, доставки, обработки и хранения электронных сообщений и документов. Как отмечают В. В. Поляков и А. В. Шебалин, компьютерные системы представляют собой совокупность технических и программных средств, используемых для формирования, приема, обработки, хранения, передачи и доставки информации. Эти средства связи представляют собой целостную электронно-вычислительную систему, в которой информация находится в электронно-цифровой форме, т.е. является компьютерной информацией[10]. Таким образом, зафиксированная информация на таких носителях в результате использования ИТС Интернет представляет собой электронно-цифровой след, под которым понимается любая криминалистически значимая компьютерная информация, т.е. (сведения, сообщения, данные), находящаяся в электронно-цифровой форме, зафиксированная на материальном носителе с помощью электромагнитных взаимодействий либо передающаяся по каналам связи посредством электромагнитных сигналов[11].

---

[9] *Бахтеев Д. В.* Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. (104). С. 43—49.

[10] *Поляков В. В., Шебалин А. В.* К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2013. № 11-1. С. 123—125.

[11] *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. Волгоград : ВА МВД России, 2008. С. 84.

При этом следует заметить, что первый и второй вид следов тесно взаимосвязаны и образуют сложную информационную систему. А самым уязвимым элементом любой системы, как верно утверждает В. С. Овчинский, является сам человек[12]. Поэтому, решая задачу по установлению пользователя ИТС Интернет, следует отталкиваться от пользовательских следов, при этом основываясь на алгоритмизированных.

Закономерно, что формирование таких следов происходит уже на этапе подключения пользователя к ИТС Интернет посредством технического устройства. Такому сетевому подключению присваивается определенное символьное значение, называемое IP-адресом. Далее при переходе пользователя на какой-либо ресурс присвоенная символьная комбинация сохраняет свое значение и фиксируется на сервере провайдера, который обеспечивает такое подключение и администратора того или иного интернет-ресурса.

С позиции техники IP-адрес представляет собой уникальный идентификатор (адрес) устройства (компьютера или иной электронно-вычислительной техники), подключенного к ИТС Интернет. То есть пользователь во время подключения к сети будет представлен идентификатором — IP-адресом, который автоматически присваивается провайдером техническому устройству, посредством которого пользователь подключается к сети. Данный идентификатор скрыт от глаз пользователя, для его обнаружения необходимо применить дополнительные манипуляции с техническим устройством либо обратиться к провайдеру с запросом.

Соответственно, органам дознания и предварительного расследования для выяснения пользователя ИТС Интернет — физического лица, предстоит совершить последовательные действия: первое — установить идентификатор (IP-адрес); второе — определить его соответствие использованному техническому устройству; третье — установить пользователя технического устройства, т.е. физическое лицо.

Пользователь ИТС Интернет осуществляет различные действия на ее ресурсах (сайтах или страницах сайтов) с присвоенным идентификатором: регистрацию на ресурсах, публикацию информации на них, пересылку файлов и различные другие действия. Кроме IP-адреса для осуществления таких действий необходимы дополнительные идентификаторы — логин/никнейм, доменное имя. Такие идентификаторы являются открытыми для широкой аудитории интернет-пользователей и не требуют дополнительных действий с техническим устройством для их обнаружения.

Из вышеизложенного следует, что пользователь и его техническое устройство могут быть представлены в ИТС Интернет такими идентификаторами, как IP-адрес, никнейм/логин, доменное имя. В связи с этим представляется необходимым уточнить, что́ входит в содержание понятия «идентификатор пользователя».

Согласно справочнику идентификатор пользователя — это символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы[13]. По нашему мнению, данное определение является довольно общим и не позволяет выявить специфику идентификаторов применительно к расследованию преступлений.

[12] *Овчинский В. С.* Криминология цифрового мира : учебник для магистратуры / М. : Норма ; Инфра-М, 2018. С. 154.

[13] URL: https://technical_translator_dictionary.academic.ru/71328 (дата обращения: 03.10.2018).

В. В. Домарев трактует идентификатор пользователя, наполняя его более подробным содержанием: символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы либо опознавание пользователя для определения его полномочий и прав на доступ к данным и выбора режима их использования. А в целом под идентификацией он понимает присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов[14].

С. В. Зуев под идентификатором понимает обозначаемый буквами ID программный элемент каскадных таблиц стилей, позволяющий назначать различный набор свойств одним и тем же физическим объектам HTML без использования классов. Такой идентификатор позволяет определить любой компьютер, в том числе с помощью IP как уникального сетевого адреса узла в компьютерной сети[15].

Анализируя определения идентификатора, которые приводятся выше, следует отметить, что он является основополагающим в таком процессе, как идентификация. Под идентификацией в криминалистике понимается процесс установления тождества объекта, его равенства самому себе, т.е. осуществления идентификации объекта по его отображению[16]. Исходя из этого, следует, что конечной целью криминалистической идентификации является установление лица по следам, обнаруженным в связи с раскрытием и расследованием преступления, что является одним из главных обстоятельств, подлежащих доказыванию по уголовному делу.

Изложенное позволяет заключить, что под *идентификатором пользователя ИТС Интернет* предлагаем понимать комбинацию символов (чисел, букв), присваиваемую сетевому подключению пользовательского (оконечного) оборудования либо задаваемую пользователем самостоятельно при использовании ИТС Интернет на конкретном ее ресурсе, позволяющую определить такое оборудование и данные лица, которое имело право его использовать.

Руководствуясь определением идентификатора пользователя, спецификой функционирования, перечисленные идентификаторы — IP-адрес, никнейм/логин, доменное имя считаем возможным разделить на две группы:

— «невидимые» идентификаторы — на примере IP-адреса;

— «видимые» идентификаторы — никнейм/логин, доменное имя.

Идентификаторы — никнейм/логин, доменное имя —являются открытыми и общедоступными в ИТС Интернет, их видят пользователи сети и для этого не требуется использования глубоких (специальных) знаний из области функционирования компьютерных технологий. Выявить и исследовать видимые идентификаторы может следователь самостоятельно, без совершения процессуальных действий, связанных с направлением запросов в соответствующие организации. Поэтому считаем, что такое разделение может быть весьма обоснованным и це-

---

[14] *Домарев В. В.* Безопасность информационных технологий. Методология создания систем защиты. Киев : ТИД ДС, 2002. С. 630.

[15] IT-справочник следователя / под ред. С. В. Зуева. М. : Юрлитинформ, 2019. С. 40.

[16] Криминалистика : учебник для прикладного бакалавриата / под ред. А. Г. Филиппова. 3-е изд., перераб. и доп. М. : Юрайт, 2017. С. 29.

лесообразным с точки зрения специфики функционирования идентификаторов и использования сведений о них для идентификации физического лица.

Далее считаем необходимым отметить, что имеющиеся научные и практические разработки в области традиционной теории криминалистической идентификации[17] не в полной мере позволяют отождествить человека — пользователя ИТС Интернет при помощи вышеназванных идентификаторов. Это связано с тем, что преступникам, использующим ИТС Интернет, свойственно стремление свести к минимуму возможность установления их личности, оставаясь максимально незамеченными в сети. Это происходит не случайно, поскольку использование ИТС Интернет в полной мере нормативно не урегулировано действующим законодательством. Кроме того, имеют место и различные программные средства, позволяющие осуществлять действия в сети анонимно, используя так называемые анонимайзеры[18]. В этой связи верно, по нашему мнению, отмечает Г. В. Скорик, что не всегда реальная и виртуальная идентичность совпадают[19].

В связи с этим следует отметить, что одной из задач Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 № 646, является исключение анонимности человека в сети Интернет. Воплощением данной Доктрины в жизнь государства стало принятие целого ряда новых и совершенствование существующих нормативных правовых актов, касающихся урегулирования процедуры идентификации пользователя в информационно-телекоммуникационных сетях.

Так, например, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обязывает организатора распространения информации в сети Интернет осуществлять «идентификацию пользователей сети Интернет, передачу электронных сообщений которых осуществляет организатор сервиса обмена мгновенными сообщениями по абонентскому номеру оператора подвижной радиотелефонной связи» (п. 1 ч. 4.2 ст. 10.1).

Доступ пользователей к информации, содержащейся в государственных информационных системах и иных информационных системах, осуществляется через Единую систему идентификации и аутентификации (ЕСИА)[20]. Для полу-

---

[17] См. например: *Колдин В. Я.* Идентификация и ее роль в установлении истины по уголовным делам. М., 1969 ; *Колмаков В. П.* Идентификационные действия следователя. М., 1977 ; *Потапов С. М.* Принципы криминалистической идентификации // Советское государство и право. М., 1940. № 1. С. 66—81 ; *Седова Т. А.* Проблемы методологии и практики нетрадиционной криминалистической идентификации. Л. : Изд-во Ленингр. ун-та, 1986. 105 с. ; *Степаненко Д. А.* Проблемы теории и практики криминалистической идентификации : дис. … д-ра юрид. наук : 12.00.09. Иркутск, 2006. 337 с.

[18] *Вехов В. Б., Ульянова М. А.* К вопросу криминалистического исследования анонимайзеров // Актуальные научные исследования в современном мире. 2018. № 7-3 (39). С. 54—57.

[19] *Скорик Г. В.* Человек в информационном обществе: проблема идентификации (поиска идентичности) // Вестник Томского государственного университета. 2007. № 302. С. 53—55.

[20] Регламентируется постановлением Правительства РФ от 28.11.2011 № 977 «О Федеральной государственной информационной системе “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое

чения учетной записи ЕСИА необходимо удостоверить свою личность с помощью паспортных данных, ИНН и СНИЛС, а также номера мобильного телефона и адреса электронной почты, являющихся идентификаторами сведений о субъектах доступа (физических и юридических лиц)[21].

В постановлении Правительства РФ от 10.09.2007 № 575 (в редакции от 25.10.2017) «Об утверждении правил оказания телематических услуг связи» указывается, что в случае заключения срочного договора об оказании разовых телематических услуг связи в пунктах коллективного доступа оператор связи[22] осуществляет идентификацию пользователей и используемого ими оконечного оборудования.

Идентификация пользователя осуществляется оператором связи путем установления фамилии, имени, отчества (при наличии) пользователя, подтверждаемых документом, удостоверяющим личность, либо иным способом, обеспечивающим достоверное установление указанных сведений, в том числе с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», или достоверного установления абонентского номера, назначенного пользователю в соответствии с договором об оказании услуг подвижной радиотелефонной связи, заключенным с оператором связи.

Идентификация оконечного оборудования осуществляется средствами связи оператора связи путем определения уникального идентификатора оборудования сетей передачи данных.

Более того, согласно данному постановлению, оператор связи может потребовать подтвердить соответствие персональных данных фактического пользователя сведениям, заявленным в договоре, осуществить подтверждение персональных данных путем представления оператору связи документа, удостоверяющего личность, или иным указанным способом.

Также о способах идентификации упоминается в Федеральном законе от 07.07.2003 № 126-ФЗ «О связи», постановлении Правительства РФ от 16.07.2007 № 447 «О совершенствовании учета федерального имущества» и др.

взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”».

Виды идентификаторов определяются в соответствии с постановлением Правительства РФ от 14.09.2012 № 928 «О базовых государственных и информационных ресурсах» и положением о федеральной государственной информационной системе “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”», утв. приказом Минкомсвязи России от 13.04.2012 № 107.

[21] Постановление Правительства РФ от 12.08.2014 № 801 «О внесении изменений в некоторые акты Правительства Российской Федерации» // СПС «КонсультантПлюс».

[22] Оператор связи оказывает телематические услуги связи, в том числе доступа к ИТС Интернет на основании договора.

В руководящем документе — Защита от несанкционированного доступа к информации. Термины и определения», утвержденного решением председателя Гостехкомиссии России от 30.03.1992, дается определение понятия «идентификация», под которой понимается присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Расшифровывается термин «идентификатор доступа» как уникальный признак субъекта или объекта доступа[23].

Исходя из вышеизложенного, следует отметить, что государственные меры, предпринимаемые для исключения анонимности пользователя в сети, могут позволять воспринимать след в ИТС Интернет как отражение человека с его истинными данными.

Однако использование сетевых технологий в раскрытии и расследовании преступлений свидетельствует о том, что в процессе установления физического лица — пользователя ИТС Интернет через идентификаторы пользователя следует учитывать, что пользовательским оборудованием, которому был присвоен идентификатор в сети, мог воспользоваться широкий круг лиц. Поэтому полагаем, что процесс сопоставления идентификатора пользователя в ИТС Интернет с реальным человеком подразумевает проведение комплекса следственных действий и оперативно-розыскных мероприятий для установления лица, использовавшего оборудование с таким идентификатором в интересующий следствие момент времени, т.е., как отмечает Г. В. Скорик, сочетание реального и виртуального способов идентификации[24].

Если в классической идентификации человека можно однозначно идентифицировать по следу руки, который он оставил на месте происшествия, при этом изучая как можно больше его частных признаков, то по следу, оставленному в ИТС Интернет также возможно говорить об индивидуальной идентификации, но не исключая ее возможный групповой характер. В данном контексте объектами групповой идентификации могут являться как законный владелец технического устройства, так и иные лица, которые могли иметь к нему доступ.

Считаем, что первоначальным алгоритмом действий субъектов уголовного преследования, направленным на установление пользователя ИТС Интернет, могут быть:

— выяснение идентификатора пользователя;
— подготовка и направление запроса провайдеру связи, администратору сайта с целью получения более подробной информации по интересующему идентификатору и техническому устройству, осуществлявшему доступ в ИТС Интернет. Получение такой информации возможно в рамках проведения следствен-

[23] См.: ФСТЭК России. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Руководящий документ. Решение председателя Гостехкомиссии России от 30.03.1992 // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 (дата обращения: 03.10.2018).

[24] *Скорик Г. В.* Указ. соч. С. 55.

ного действия, предусмотренного ст. 186.1 УПК РФ (получение информации о соединениях между абонентами и (или) абонентскими устройствами);
— допрос владельца пользовательского оборудования;
— установление круга лиц, имеющего доступ к пользовательскому оборудованию, их допрос;
— выемка и осмотр видеозаписей вблизи того географического места, откуда осуществлялось подключение к ИТС Интернет для отслеживания местоположения лиц, имевших доступ в сеть в интересующий следователя момент времени;
— обыск места, откуда производился доступ в ИТС Интернет пользователем;
— осмотр пользовательского оборудования;
— назначение экспертиз (компьютерно-техническая, лингвистическая, судебно-медицинская вещественных доказательств и проч.).

Среди оперативно-розыскных мероприятий, направленных на установление пользователя ИТС Интернет, причастного к подготовке и совершению преступлений, считаем необходимым указать следующие:
— наведение справок, предполагающее получение из различных учреждений сведений о пользователе, а также данных из открытых источников информационных ресурсов;
— сбор образцов для сравнительного исследования, предполагающий получение объектов — носителей информации, необходимых для их исследования путем изучения, описания, сравнения с ранее добытыми объектами;
— получение компьютерной информации;
— негласное наблюдение — оперативно-розыскное мероприятие, осуществляемое в сетях передачи информации с использованием специальных технических средств и фиксацией (или без нее) результатов для получения сведений, имеющих значение для решения задач оперативно-розыскной и уголовно-процессуальной деятельности;
— оперативное внедрение, открывающее широкие возможности для обнаружения, изучения, фиксации информационных объектов;
— оперативный эксперимент — оперативно-розыскное мероприятие, направленное на моделирование определенных информационных объектов и отношений, возникающих в противоправных действиях ее субъектов[25].

Таким образом, при успешном взаимодействии следственных и оперативных подразделений, тактически верном разделении обязанностей по поставленным задачам, а также умелом использовании интернет-ресурсов станет возможным решить задачу, связанную с установлением личности пользователя, осуществляющего неправомерные действия. Безусловно, количество и порядок осуществления следственных действий и оперативно-розыскных мероприятий будет зависеть от сложившейся следственной ситуации по делу в целом и варьироваться исходя из объема имеющихся данных.

---

[25] *Ищенко Е. П.* О некоторых подходах к выявлению и расследованию преступлений, совершаемых в виртуальном пространстве // О криминалистике и не только : избранные труды. М. : Проспект, 2016. С. 14—23.

Так или иначе, но повсеместное внедрение информационно-телекоммуникационных технологий в противоправную деятельность позволяет констатировать, что поисково-познавательную деятельность сотрудников, осуществляющих расследование, необходимо совершенствовать путем расширения использования такого источника информации, как ИТС Интернет, в частности, для решения задачи идентификации пользователя — физического лица.

Таким образом, подводя итог изложенному, считаем возможным заключить следующее.

1. Имеющиеся научные и практические разработки в области традиционной криминалистической идентификации не в полной мере позволяют осуществлять идентификацию человека, представленного в ИТС Интернет посредством идентификаторов. Это обусловливает необходимость установления идентификаторов пользователя ИТС Интернет и их принадлежности техническому устройству, которое использовало физическое лицо при подготовке, совершении и сокрытии преступления, т.е. идентифицировать данное лицо.
2. Под идентификатором пользователя ИТС Интернет предлагается понимать комбинацию символов (чисел, букв), присваиваемую сетевому подключению пользовательского (оконечного) оборудования либо задаваемую пользователем самостоятельно при использовании ИТС Интернет на конкретном ее ресурсе, позволяющую определить такое оборудование и данные лица, которое имело право его использовать.
3. Руководствуясь определением идентификатора пользователя, спецификой функционирования, перечисленные идентификаторы — IP-адрес, никнейм/логин, доменное имя — целесообразно разделить на две группы:
   — «невидимый» идентификатор — IP-адрес;
   — «видимые» идентификаторы — никнейм/логин, доменное имя.
4. Повсеместное внедрение информационно-телекоммуникационных технологий в противоправную деятельность позволяет констатировать, что поисково-познавательную деятельность сотрудников, осуществляющих расследование, необходимо совершенствовать путем расширения использования такого источника информации, как ИТС Интернет, в частности, для решения задачи идентификации пользователя — физического лица.

БИБЛИОГРАФИЯ

1. *Аверьянова Т. В., Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов / под ред. Р. С. Белкина. — 2-е изд., перераб. и доп. — М. : Норма, 2005. — 992 с.
2. *Балашов Д. Н., Балашов Н. М.*, *Маликов С. В.* Криминалистика : учебник. — 2-е изд. — М. : Инфра-М, 2009. — 503 с.
3. *Бахтеев Д. В.* Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. — 2018. — № 2. (104). — С. 43—49.
4. *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. — Волгоград : ВА МВД России, 2008. — 401 с.

5. *Вехов В. Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. — 2016. — № 1 (11). — С. 155—158.
6. *Вехов В. Б., Ульянова М. А.* К вопросу криминалистического исследования анонимайзеров // Актуальные научные исследования в современном мире. — 2018. — № 7—3 (39). — С. 54—57.
7. *Домарев В. В.* Безопасность информационных технологий. Методология создания систем защиты — Киев : ТИД ДС, 2002. — 688 с.
8. *Ищенко Е. П.* Актуальные направления развития криминалистики // Актуальные вопросы криминалистики и уголовно-процессуального права : мат. конф. — Киров, 2005. — С. 7—11.
9. *Ищенко Е. П.* О некоторых подходах к выявлению и расследованию преступлений, совершаемых в виртуальном пространстве // О криминалистике и не только : избранные труды. — М. : Проспект, 2016. — С. 14—23.
10. *Ищенко Е. П.* Российская криминалистика сегодня // О криминалистике и не только : избранные труды. — М. : Проспект, 2016. — С. 38—46.
11. *Колдин В. Я.* Идентификация и ее роль в установлении истины по уголовным делам. — М., 1969.
12. *Колмаков В. П.* Идентификационные действия следователя. — М., 1977.
13. Криминалистика : учебник / отв. ред. Н. П. Яблоков. — 3-е изд., перераб. и доп. — М. : Юристъ, 2005. — 781 с.
14. Криминалистика : учебник для прикладного бакалавриата / под ред. А. Г. Филиппова. — 3-е изд., перераб. и доп. — М. : Юрайт, 2017. — 466 с.
15. Криминалистика : учебник для экспертов-криминалистов / под ред. А. Г. Филиппова. — М. : Юрлитинформ, 2005. — 484 с.
16. *Мочагин П. В.* Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе // Вестник Удмуртского университета. Серия «Экономика и право». 2013. № 2. С. 148—154.
17. *Овчинский В. С.* Криминология цифрового мира : учебник для магистратуры. — М. : Норма ; Инфра-М, 2018. — 352 с.
18. *Поляков В. В., Шебалин А. В.* К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. — 2013. — № 11—1. — С. 123—125.
19. *Потапов С. М.* Принципы криминалистической идентификации // Советское государство и право. — 1940. — № 1. — С. 66—81.
20. *Седова Т. А.* Проблемы методологии и практики нетрадиционной криминалистической идентификации. — Л. : Изд-во Ленингр. ун-та, 1986. — 105 с.
21. *Скорик Г. В.* Человек в информационном обществе: проблема идентификации (поиска идентичности) // Вестник Томского государственного университета. — 2007. — № 302. — С. 53—55.
22. *Степаненко Д. А.* Проблемы теории и практики криминалистической идентификации : дис. … д-ра юрид. наук : 12.00.09. — Иркутск, 2006. — 337 с.
23. IT-справочник следователя / под ред. С. В. Зуева. — М. : Юрлитинформ, 2019. — 232 с.