УДК 343.9, ББК 67.629.4 © К.С. Сидорова

К.С. Сидорова

СПОСОБЫ УСТАНОВЛЕНИЯ IP-АДРЕСА И СВЕДЕНИЙ О НЕМ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ

В статье предлагается перечень способов по установлению IP-адреса и сведений о нем в ходе расследования преступлений. Излагается сущность следующих способов по установления IP-адреса для получения сведений о нем: направление запроса в адрес компании-провайдера, осуществляющей услуги доступа к сети «Интернет» по определенному физическому адресу; направление запроса администрации сайта, на котором зарегистрирован интересующий следователя (дознавателя) пользователь в рамках расследования уголовного дела; проведение следственных действий с целью установления IP-адреса; направление поручения органу дознания об установлении IP-адреса конкретного соединения (й) по обстоятельствам совершенного преступления. Так как по IP-адресу возможно идентифицировать техническое устройство, посредством которого осуществлялся доступ в сеть «Интернет», а в последующем и физическое лицо, это обязывает следователя (дознавателя) устанавливать такого рода сведения для проверки о причастности лица к совершенному преступлению. Полученная информация поможет следователю (дознавателю) спланировать дальнейший ход расследования и проверить ранее выдвинутые версии и проверить вновь возникшие. Отмечается, что сведения, содержащиеся в ответе организации-провайдера, исходя из содержания ст. 74 УПК РФ могут быть отнесены к такой категории доказательств, как иные документы.

Подчеркивается, что перечисленные способы установления IP-адреса и сведений о нем не являются исчерпывающими. Рассмотрены лишь наиболее часто встречающиеся способы. Решение об использовании того или иного способа принимается исходя из конкретной следственной ситуации и зависит от обстоятельств совершенного преступления и объема имеющейся информации по делу в целом. В ходе исследования применялись следующие методы: диалектический, анализ, дедукция, обобщение. Результаты исследования применимы сотрудниками подразделений следствия и дознания, специалистами в области криминалистики

Ключевые слова: методика расследования отдельных видов и групп преступлений, информационные технологии, следователь (дознаватель), IP-адрес, идентификация, техническое устройство, запрос, провайдер, поручение.

В настоящее время сеть «Интернет» представляет собой многогранное информационное пространство, которое предоставляет человеку широкие возможности по его использованию. Население активно пользуется различными услугами в сети «Интернет»: регистрируется на официальных сайтах с целью получения какой-либо государственной услуги, общается на сайтах социальных сетей, совершает покупки в режиме «онлайн» на сайтах продаж. Данный процесс, безусловно, сопровождается следами пребывания физического лица в сети «Интернет». Если в действительности человека идентифицируют по следам обуви, транспортных средств, голосу, то в виртуальном пространстве представляется возможным это делать по неким идентификаторам в сети «Интернет», которыми представлен пользователь в сети и техническое устройство, благодаря которому он осуществляет активные действия в сети. Изучение таких идентификаторов необходимо и требует как научной проработки, так и практической, с целью идентификации физического лица и технического устройства по определенному идентификатору.

Одним из таких «невидимых» для глаз пользователя, не владеющего специальными знаниями в области информационных технологий, является IP-адрес. Сведения о нем представляют значительный массив криминалистически значимой информации. Такие данные, по нашему мнению необходимо устанавливать, когда в процессе совершения преступления были задействованы ресурсы сети «Интернет» с целью подтверждения причастности лица к преступлению. Причем, вне зависимости от того, каким образом они были задействованы в преступлении – как орудие преступления [2], либо же, как средство связи [3]. В результате таких действий формируются следы, которые могут отражать элементы механизма преступной деятельности, и в то же время являться ориентирующей для следователя информацией. Как справедливо отмечает Е.П. Ищенко, открытость и глобальность Интернета, например, представляющего собой всемирную телекоммуникационную сеть, образованную путем объединения более 10 500 телекоммуникационных сетей разных типов, создают огромные потенциальные возможности для более активного использования новых информационных технологий в целях раскрытия и расследования совершаемых в стране преступлений [4, с. 9]. Таким образом, с целью всестороннего изучения всех обстоятельств уголовного дела, а также получения как ориентирующей, так и доказательственной информации, возникает необходимость установления IP-адреса, а в последующем и сведений о нем и использования в деятельности по расследованию преступлений.

Начальным этапом использования IP-адреса с целью получения сведений о нем в расследовании преступлений, является установление самого IP-адреса. Существуют следующие способы установления IP-адреса: 1) направление запроса в

адрес компании-провайдера, осуществляющей услуги доступа к сети «Интернет» по определенному физическому адресу; 2) направление запроса администрации сайта, на котором зарегистрирован интересующий следователя пользователь в рамках расследования уголовного дела; 3) проведение следственных действий с целью установления IP-адреса; 4) направление поручения органу дознания об установлении IP-адреса конкретного соединения (й) по обстоятельствам совершенного преступления.

Первый способ. В рамках данного способа первоначально необходимо направить запрос в адрес управляющей организации по месту проживания интересующего лица для установления всех провайдеров, предоставляющих услуги доступа к сети «Интернет» по конкретному географическому адресу. Следует отметить, что в соответствии с ч. 4 ст. 21 УПК РФ мотивированный запрос следователя подлежит обязательному исполнению всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами, в том числе и компанией-провайдером, осуществляющим услуги доступа к сети «Интернет». Предполагается, что ответ управляющей организации должен содержать сведения о наименовании провайдеров, с которыми были заключены договоры о предоставлении доступа к услугам сети «Интернет» по адресу, указанному в запросе. После получения ответа должны быть направлены запросы по адресам установленных организаций-провайдеров о предоставлении следователю следующей информации:

— полные данные, указанные лицом при заключении договора об оказании услуг связи, в том числе, доступа к сети «Интернет» (фамилия, имя, отчество, адрес, телефон, копия паспорта + копия договора);

— используемые пользователем IP-адреса в период времени (следователем указывается точный промежуток времени, который его интересует в формате час, минута, секунда);

— вид используемого IP-адреса (статический или динамический);

— адрес местонахождения приемопередающего оборудования, по средствам которого осуществлялся выход в сеть «Интернет», через указанные IP-адреса;

— используемые в определенный промежуток времени MAC-адреса;

— иные сведения, которые содержатся у провайдера по поводу данного пользователя и подключений, которые им осуществлялись в указанный промежуток времени.

Предполагаем, что такой ход действий – путем направления официального запроса в адрес управляющей компании не исключает того, что может последовать преждевременное нежелательное распространение информации, имеющей значение для расследования уголовного дела, а также иметь место затягивание сроков расследования в связи с несвоевременным ответом на запрос. Для того чтобы не допустить разглашения информации и увеличения сроков расследования, с тактической точки зрения, следователю надлежит установить с помощью интернет-ресурсов всех провайдеров, предоставляющих услуги доступа к сети «Интернет» по конкретному адресу, после чего выяснить у сотрудников компании-провайдера какая из них осуществляет доступ по определенному адресу. В адрес искомой организации-провайдера направить запрос с требованием сообщить сведения, указанные выше.

Полученная информация, содержащаяся в ответе организации-провайдера, исходя из содержания ст. 74 УПК РФ, по нашему мнению, может быть отнесена к такой категории доказательств, как иные документы. Кроме того, мы полагаем, если такой документ будет довольно объемным по содержанию, то целесообразно его осматривать в рамках осмотра и отмечать в протоколе наиболее существенные и имеющие значение факты для расследования преступного события.

Нельзя не отметить того, что запрос в организацию-провайдер необходимо направлять одновременно с постановлением суда о разрешении получения такой информации. Сведения, полученные от провайдера, содержат персональные данные лица, на имя которого оформлен договор об оказании услуг доступа к сети «Интернет», информацию о соединениях пользовательского оборудования с сетью «Интернет», получение которой осуществляется в порядке ст. 165 УПК РФ в рамках такого следственного действия, предусмотренного статьей 186 УПК РФ, как «Получение информации о соединениях между абонентами и (или) абонентскими устройствами».

Более того, считаем, что в целях соблюдения оптимальных сроков расследования уголовных дел, а также с целью дисциплинированности провайдеров связи и оперативного получения ответа на исходящий запрос от следователя (дознавателя), считаем необходимым в нем указывать, что в случае не предоставления или несвоевременного предоставления запрашиваемой информации, виновное лицо может быть привлечено к административной ответственности в соответствии со ст. 17.7 Кодекса об Административных правонарушениях РФ «Невыполнение законных требований прокурора, следователя, дознавателя или должностного лица, осуществляющего производство по делу об административном правонарушении».

Второй способ. В настоящее время сеть «Интернет» и ее ресурсы используются как в правомерных целях, так и с целью совершения преступлений. Для осуществления этих действий, пользователь регистрируется на различных сайтах, указывая при этом свои персональные данные. В результате этого, пользователь использует в ходе работы на сайте после регистрации никнеймы/ники/логины, идентификационные номера и другие «видимые» идентификаторы. Таким образом, фиксируется техническая составляющая подключения к

сети «Интернет» по конкретному идентификатору в виде IP-адресов, по которым получается необходимая для следователя информация. При этом нельзя не отметить, как положительное явление, способствующее повышению эффективности расследования уголовных дел, дальнейшее совершенствование нормативно-правовой базы, регламентирующей хранение такой информации. Так, например, государство обязало организаторов распространения информации хранить на территории РФ информацию о гражданах РФ, регистрирующихся на различных сайтах и мессенджерах, серверы которых могут находиться и за пределами РФ, установили и сроки хранения информации о пользователях РФ. Согласно пп. 2 п. 3 ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации», организатор распространения информации в сети «Интернет» обязан хранить на территории РФ – текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки, а информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий [1].

Полагаем, что, установив сайт, на котором зарегистрирован пользователь – интересующее орган расследования физическое лицо, следует направить запрос в администрацию этого сайта с требованием предоставить:

— данные, которые указывало лицо при регистрации аккаунта на определенном сайте (ФИО, телефон, электронную почту и иную информацию);

— IP-адреса и интенсивность посещения сайта в определенный промежуток времени.

В данном случае, также необходимо получать постановление суда о разрешении получения такой информации, так как она будет составлять персональные данные пользователя. Поскольку статья 7 Федерального закона «О персональных данных», обязывает операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

После этого, установив такие сведения, следует выяснять наименование провайдера, в сети которого зарегистрирован установленный IP-адрес и его географическое местоположение.

В решении этой задачи могут помочь интернет-ресурсы – «WHOIS», «2IP», «RIPE» и другие, которые располагают сведениями об IP-адресах. При запросе об IP-адресе или доменном имени на таких сайтах, выдается информация о стране, городе, названии провайдера.

Примечательно, что деятельность данных сайтов со стороны государства не контролируется, но проанализировав пользовательские соглашения вышеперечисленных сайтов, следует, что их функционирование построено в соответствии с требованиями действующего российского законодательства и направлено на регулирование взаимоотношений между Администрацией, пользователями сайта и провайдерами (права, обязанности, пределы ответственности). Между пользователем сайта и администрацией заключается договор, регламентированный ст. 428 Гражданского кодекса РФ в режиме онлайн. В соответствии с данной нормой, условия договора устанавливаются в одностороннем порядке Администрацией сайта и содержатся в Пользовательском соглашении (правилах пользования сайтом). В соответствии с данной нормой ГК РФ и Пользовательским соглашением, Пользователи сайта могут направить свои обращения, предложения и претензии к Администрации сайта. В случае недостижения согласия, споры, связанные с исполнением гражданско-правового договора, разрешаются в судебном порядке по заявлению заинтересованной стороны.

Кроме того, в пользовательских соглашениях данных сайтов отмечается, что в случае неточностей, недостоверности, необъективности предоставляемых данных с таких сайтов, а также отклонений в части качества оказания услуг, администрация сайта ответственности не несет. В связи с этим возникает вопрос относительно степени доверия правоохранительных органов к сведениям, размещаемым на таких сайтах. Нельзя не согласиться с А.Н. Першиным, по мнению которого сведения из неофициальных источников не позволяют использовать их как единственный источник доказательственной информации и требуют применения системы процессуальных и криминалистических мер проверки изложенных в них фактов [6, с. 57].

В целях проверки информации об IP-адресе, полученной из указанных интернет-ресурсов и дальнейшего ее использования в качестве доказательства по уголовному делу, считаем целесообразным направлять запросы в соответствующие организации провайдера, в диапазоне которого находится необходимый IP-адрес об установлении факта принадлежности или непринадлежности определенного IP-адреса диапазону IP-адресов, имеющихся у провайдера.

Третий способ. Осмотр предмета (в нашем случае это компьютер, планшет, смартфон и другие устройства, с которых был выход в сеть «Интернет») является распространенным следственным действием. Для повышения эффективности осмотра электронного вычислительного устройства целесообразно привлекать специалиста. Следует

учитывать, что место размещения информации об IP-адресе на разных видах устройств отличается:

— при осмотре компьютеров: панель управления→центр управления сетями и общим доступом→активное сетевое соединение→сведения, где одним из пунктов будет цифровое значение IP-адреса;

— при осмотре смартфонов и других портативных устройств связи: настройки→общие→о телефоне→сеть, где одним из пунктов будет цифровое значение IP-адреса.

Следует отметить, что в целях сохранения всех сведений на электронном носителе и исключения их дальнейшего изменения, предлагается изымать электронный носитель информации с целью проведения компьютерной экспертизы. Производить такое действие возможно как в ходе осмотра, так и в ходе обыска, выемки [5; 8]. Выбор того или иного следственного действия будет обусловлен сложившейся следственной ситуацией и объемом сведений, которые предполагается получить. В случае необходимости установления на носителе только используемых IP-адресов допустимо ограничиться и проведением осмотра с привлечением специалиста.

Четвертый способ. Поручение органу дознания об установлении IP-адреса конкретного соединения (й) по обстоятельствам совершенного преступления может быть вызвано необходимостью более оперативного получения информации иными службами в случае, когда промедление может привести к утрате информации, либо объективной невозможностью проведения необходимые мероприятия в кратчайшие сроки следователем. Более того, применение такого способа установления IP-адреса может быть связано с необходимостью проведения специальных технических мероприятий негласным способом. Разумеется, данное решение должно быть обоснованным и необходимым и соответствовать целям расследования [7, с. 290].

Авторское достижение состоит в выделении критериев формулирования способов установления IP-адреса и сведений о нем, основанных на аспектах процессуальной и непроцессуальной деятельности следователя, криминалистической и следственной ситуации до - и пост - криминального поведения виновного лица, технических возможностях и целесообразности их использования на конкретном этапе расследования деяния. В результате изучения теоретических источников и практики расследования уголовных дел различной категории нами были выделены четыре способа установления IP-адреса и сведений о нем. В обобщенном виде их можно представить следующим образом: направление запроса провайдеру; направление запроса администратору сайта; проведение специальных следственных действий; направление поручения.

Итак, решение об использовании того или иного способа принимается исходя из конкретной следственной ситуации и зависит от обстоятельств совершенного преступления и объема имеющейся информации по делу в целом. Вместе с тем перечень изложенных способов по установлению IP-адреса не является исчерпывающим, нами рассмотрены лишь наиболее часто встречающиеся способы.

Библиографический список

1. Подпункт 2 пункта 3 статьи 10.1 вступает в силу с 1 июля 2018 года (Федеральный закон от 06.07.2016 N 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»).

2. Росправосудие [электронный ресурс] / Приговор Ленинского районного суда г. Чебоксары Чувашской Республики от 8 августа 2016 года по делу № 1–356/2016. – Режим доступа: https://rospravosudie.com/court-petropavlovsk-kamchatskij-gorodskoj-sud-kamchatskij-kraj-s/act-560786355/, свободный.

3. Росправосудие [электронный ресурс] / Приговор Петропавловск-Камчатского городского суда Камчатского края от 14 июля 2016 года по делу № 1–388/2016. – Режим доступа: https://rospravosudie.com/court-petropavlovsk-kamchatskij-gorodskoj-sud-kamchatskij-kraj-s/act-533001459/, свободный.

4. Ищенко, Е.П. Криминалистика и новые информационные технологии [текст] / Е.П. Ищенко // Вестник криминалистики. – 2009. – № 3 (31). – 212 с.

5. Казначей, И.В. Проблемные аспекты изъятия с участием специалиста электронных носителей информации при производстве по уголовным делам [текст] / И.В. Казначей // Судебная экспертиза. – 2013. – № 2 (34). – С. 14-20;

6. Першин, А.Н. Анализ как метод познания документированной информации [текст] / А.Н. Першин // Научный вестник Омской академии МВД России. – 2014. – № 3. – С. 54–58.

7. Седельников, П.В. Обоснованность направления поручения органу дознания следователем [текст] / П.В. Седельников // Сборник материалов XXII международной научно-практической конференции в 2 т. – Иркутск, 2017. – С. 290–293.

8. Шигуров, А.В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации [текст] / А.В. Шигуров // Библиотека криминалиста. – 2013. – № 5 (10). – С. 135–140.

References

1. Subparagraph 2 of paragraph 3 of Article 10.1 shall enter into force on July 1, 2018 (Federal Law of July 6, 2016 No. 374-FZ «On Amendments to the Federal Law «On Counteracting Terrorism» and certain legislative acts of the Russian Federation with regard to the establishment of additional measures counteraction to terrorism and ensuring public security»).

2. Justice [electronic resource] / The verdict of the Leninsky District Court of Cheboksary of the Chuvash Republic of August 8, 2016 in case No. 1–356 / 2016. – Access mode: https://rospravosudie.com/court-petropavlovsk-kamchatskij-gorodskoj-sud-kamchatskij-kraj-s/act-560786355/, free.

3. Justice [electronic resource] / The verdict of the Petropavlovsk-Kamchatsky city court of the Kamchatka Territory of July 14, 2016 in case No. 1–388 / 2016. – Access mode: https://rospravosudie.com/court-petropavlovsk-kamchatskij-gorodskoj-sud-kamchatskij-kraj-s/act-533001459/, free.

4. Ishhenko E.P. *Kriminalistika i novye informacionnye tehnologii* [Forensic science and new information technologies]. Herald of Forensic Science. 2009. No. 3 (31). 212 p.

5. Kaznachej I.V. *Problemnye aspekty iz#jatija s uchastiem specialista jelektronnyh nositelej informacii pri proizvodstve po ugolovnym delam* [The problematic aspects of the withdrawal with the participation of a specialist, of electronic media in criminal proceedings]. Forensic examination. 2013. No. 2 (34). P. 14–20;

6. Pershin A.N. *Analiz kak metod poznanija dokumentirovannoj informacii* [Analysis as a method of cognition of documented information]. The scientific bulletin of Omsk academy of the Ministry of Internal Affairs of Russia. 2014. No 3. P. 54–58.

7. Sedel'nikov P.V. *Obosnovannost' napravlenija poruchenija organu doznanija sledovatelem* [Justification of the direction of the commission to the investigating body by the investigator]. Collection of materials of the XXII international scientific-practical conference in 2 t. Irkutsk, 2017. P. 290–293.

8. Shigurov A.V. *Problemy regulirovanija porjadka provedenija sledstvennyh dejstvij, soprovozhdajushhihsja iz#jatiem jelektronnyh nositelej informacii* [The problems of regulating the procedure for conducting investigative actions, accompanied by the withdrawal of electronic media]. Forensic library. 2013. No. 5 (10). P. 135–140.

METHODS OF INSTALLING IP-ADDRESS AND INFORMATION ABOUT IT IN THE INVESTIGATION OF CRIMINAL PROCEEDINGS

Kseniya S. Sidorova,
The Post-graduate student, Omsk Academy of the RF Ministry of Internal Affairs

Abstract. The article suggests a list of ways to establish an IP-address and information about it during the investigation of crimes. The essence of the following methods for establishing an IP-address for obtaining information about it is stated: sending a request to the provider company that provides Internet access services at a certain physical address; sending a request to the administration of the site where the user of the investigator (inquirer) interested in the investigation of the criminal case is registered; conducting investigative actions to establish an IP-address; sending a request to the inquiry agency to establish the IP-address of a particular connection (s) for the circumstances of the crime committed. Since it is possible to identify by an IP-address a technical device through which access to the Internet network was made, and subsequently an individual, this obliges the investigator (inquirer) to establish such information to verify the person's involvement in the committed crime . The information obtained will help the investigator (the investigator) to plan the further course of the investigation and check the previously submitted versions and check the newly emerged ones. It is noted that the information contained in the response of the provider organization, based on the content of Art. 74 of the Code of Criminal Procedure can be assigned to this category of evidence, as other documents.

It is emphasized that the listed ways of establishing an IP-address and information about it are not exhaustive. Only the most frequently encountered methods are considered. The decision to use this or that method is taken based on a specific investigative situation and depends on the circumstances of the committed crime and the amount of information available in the case as a whole. The study used the following methods: dialectical, analysis, deduction, generalization. The results of the study are applicable to investigative units, specialists in the field of forensic science.

Key words: methods of the investigation of certain types and groups of crimes, information technology, investigator, IP-address, identification, technical device, request, provider, assignment.

Сведения об авторе:

Сидорова Ксения Сергеевна – адъюнкт адъюнктуры ФГКОУ ВО «Омская академия Министерства внутренних дел Российской Федерации» (644092, Российская Федерация, г. Омск, пр. Комарова, д. 7), e-mail: k_s159@mail.ru.

Статья поступила в редакцию 27.03.2018 г.