Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2022, 3: 161–167

EDN NQHPPZ
DOI 10.26163/GIEF.2022.31.84.023
УДК 343.133:(349:004.9)

Р.А. Рамазанов

ОСОБЕННОСТИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА И ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Рамин Анатольевич Рамазанов – доцент кафедры управления социальными и экономическими процессами, Государственный институт экономики, финансов, права и технологий, кандидат педагогических наук, г. Гатчина; **e-mail: ramaha2007@mail.ru**.

В статье выявляются и анализируются особенности возбуждения уголовного дела и первоначального этапа расследования преступлений в сфере информационно-телекоммуникационных технологий. Рассмотрен порядок проведения проверочных мероприятий и процессуальных действий при расследовании преступлений данной категории.

***Ключевые слова**: возбуждение уголовного дела; оперативно-розыскные мероприятия; информационно-телекоммуникационные технологии; IP-адрес; Интернет; провайдер.*

R.A. Ramazanov

SPECIFICS OF INITIATION OF CRIMINAL PROCEEDINGS AND FEATURES OF INITIAL STAGE OF IT CRIMES INVESTIGATION

Ramin Ramazanov – Associate Professor, the Department of Management of Social and Economic Processes, State Institute of Economics, Finance, Law and Technology, PhD in Pedagogics, Gatchina; **e-mail: ramaha2007@mail.ru**.

The article reveals and analyses specifics of the initiation of criminal proceedings and particulars of the initial stage of the investigation of crimes in the field of information and telecommunication technologies. The procedure for conducting verification activities and procedural actions to be performed in the course of investigation of crimes of this category is considered.

***Keywords**: initiation of criminal proceedings; operational search measures; information and telecommunication technologies; IP address; Internet; provider.*

Задача стадии возбуждения уголовного дела – выявление поводов и основания для возбуждения уголовного дела, в соответствии с которыми орган дознания, дознаватель или следователь в пределах компетенции и в зависимости от результатов проверки принимают решение о возбуждении уголовного дела. Возбуждение уголовного дела служит начальным этапом уголовного процесса. На данном этапе принимается сообщение о преступлении, проводятся проверочные мероприятия, производится анализ результатов (полученной информации) относительно допустимости и достоверности доказательств, в том числе использование в доказывании

результатов оперативно-розыскной деятельности.

В Федеральном законе от 2 мая 2006 г. № 59 «О порядке рассмотрения обращений граждан Российской Федерации» определены общие вопросы подачи и рассмотрения обращений граждан, реализующих свое право на обращение в государственные органы и органы местного самоуправления, а также к должностным лицам. Приказ от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений» имеет общий характер для правоохранительных органов. В первом приложении введено типовое положение о едином порядке организации приема регистрации и проверки сообщений о преступлении.

Заявление о компьютерных преступлениях, согласно ст. 141 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), может быть подано как в устной, так и в письменной форме, подписано заявителем и лицом, принявшим заявление. Заявитель также предупреждается об уголовной ответственности за заведомо ложный донос (ст. 306 Уголовного кодекса РФ).

С учетом судебной практики (определение Конституционного Суда РФ от 16 июля 2013 г. № 1156-О) становится очевидным, что получение сведений об IP-адресах, с которых осуществляется выход в сеть Интернет, согласно ч. 1 ст. 144 УПК РФ, является правом дознавателя, органа дознания, следователя, руководителя следственного органа при проверке сообщения о преступлении. Помимо прочего, право истребовать документы и предметы реализуется по основаниям и в порядке, установленным другими нормами УПК РФ и иными законодательными актами, а потому данное положение также не может расцениваться как ограничивающее право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [4].

При проведении процессуальных действий по проверке сообщения о данном преступлении особое внимание уделяют осмотру места происшествия, осмотру компьютера, устройства потерпевшего. Проведение осмотра с письменного согласия потерпевшего для фиксации всей информации на его устройстве, копирование всей информации для обнаружения признаков преступления по ст. 272, 273, 274, 274.1, 159.6 УК РФ. Согласно п. 3 ч. 2 ст. 151 «Подследственность» УПК РФ, ст. 272, 273, 274, 159.6 УК РФ (ч. 2–4) процессуальные действия производятся следователями органов внутренних дел. Согласно п. 2 ч. 2 ст. 151 УПК РФ, ст. 274.1 УК РФ предварительное следствие производится следователями органов федеральной службы безопасности.

В первую очередь должна быть выполнена фиксация информации, которая может безвозвратно исчезнуть (например, информация в оперативной памяти, в том числе загруженные страницы сайта в сети Интернет), при этом желательно производить фиксацию на видео- или фотоаппаратуре при проведении осмотра места происшествия. Первичное построение части схемы предположительного механизма преступления – это описание схемы по предложенной ранее классификации обнаруженных электронно-цифровых следов. К примеру, существует устройство потерпевшего, и его отнесли к личному устройству, если другие члены семьи им не пользуются. Требуется взять письменное согласие на копирование информации с устройства потерпевшего. В случае использования устройства другими членами семьи следует взять у каждого члена семьи письменное согласие на копирование информации, находящейся на устройстве. Далее фиксируется информация, содержащаяся в компьютере, причем сначала на энергозависимой части устройства, чтобы безвозвратно не потерять значимую информацию, затем на жестком диске устройства.

Стоит уточнить, что на практике пользователи сначала несколько раз пытаются войти в свой аккаунт либо своими силами устранить, как они думают, неисправность устройства, неоднократно перегружая свое устройство, тем самым безвозвратно уничтожая компьютерную информацию, находящуюся в оперативной памяти устройства – компьютера.

Заявление о преступлениях в сфере компьютерной информации от организации принимается у уполномоченных лиц, то есть от руководителя организации. Заявление должно содержать не предположение о преступлении, а утверждение. К примеру, ст. 272 УК РФ предусматривает неправомерный доступ. Поэтому в заявлении должно быть отражено не предположение о неправомерном доступе, а факт неправомерного доступа, подтвержденный данными IP-адреса, временем входа в аккаунт, фактом изменения, копирования, удаления защищенной законом или создателем компьютерной информации, которую можно будет запросить у администрации данного сетевого ресурса, где зарегистрирована данная учетная запись. По контактной информации, расположенной на данном ресурсе, как правило, указывается электронная почта. В ответ администрация ресурса запросит информацию для идентификации законного пользователя учетной записи. К примеру, нужно указать телефонный номер пользователя, который привязан к учетной записи, или адрес электронной почты.

В 2020 г. прослеживалась значительная латентность таких преступлений, во многом обусловленная возможностью преступников оставаться анонимными, избегать непосредственного контакта с потерпевшими, широкой аудиторией пользователей информационных ресурсов, упрощением доступа к ним, а также организованным и трансграничным характером подобных деяний. По данным АО «Лаборатория Касперского», с ноября 2019 г. по октябрь 2020 г. их защитные решения и защитные технологии отразили 666 809 967 атак с онлайн-ресурсов, распознали 173 335 902 вредоносных URL-адреса, заблокировали 33 412 568 вредоносных объектов, справились с 549 301 атакой вымогателей и 668 619 попытками заражения вредоносными программами, многие из которых имеют признаки преступлений, соответствующих ст. 272 и 273 УК РФ [1].

В контексте ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ наличие вредоносной программы на устройстве потерпевшего либо компьютерах организации подтверждается судебной экспертизой. Выявляется наличие следов, изменение, копирование, удаление компьютерной информации, что защищено законом или создателем вследствие результатов работы вредоносной программы. Ввиду распространения вирусного программного обеспечения злоумышленниками через сеть Интернет с использованием разного типа проникновения в устройства пользователей, к примеру, использованием «фишинга» и социальной инженерии для манипулирования действиями пользователя, необходимо при выявлении тела исполняемого файла вредоносной программы на устройстве пользователя доказать умысел использования вредоносной программы, чтобы исключить ситуацию, в которой пользователь сети Интернет оказывается жертвой злоумышленников, а его устройство без его согласия применено злоумышленниками для реализации преступного умысла.

Относительно ст. 274 УК РФ необходимым условием является установление факта наличия следов изменения, копирования, удаления компьютерной информации, защищенной законом или создателем, причинившее ущерб свыше миллиона рублей вследствие умышленного нарушения правил эксплуатации средств хранения, обработки и передачи. Факт наличия правил эксплуатации, а также ущерба свыше миллиона рублей играет ключевую роль. Без них нет состава преступления.

Статья 274.1 УК РФ предусматривает установление факта наличия следов изменения, копирования, удаления компьютерной информации, защищенной законом или создателем, находящейся в критической информационной инфраструктуре вследствие нейтрализации средств защиты; распространения, использования, создания компьютерных программ либо иной компьютерной информации; неправомерного доступа; нарушения правил эксплуатации, средств хранения обработки, передачи компьютерной информации (действия, бездействия).

Применительно к ст. 159.6 УК РФ устанавливают наличие следов изменения, копирования, удаления компьютерной информации, защищенной законом или создателем, иного вмешательства в работу средств хранения обработки или передачи компьютерной информации, повлекшее хищение чужого имущества. Обязательное условие – наличие заявления потерпевшего, поскольку возбуждение уголовного дела частно-публичного обвинения о преступлении, совершенном индивидуальным предпринимателем в связи с осуществлением предпринимательской деятельности и/или управлением принадлежащим ему имуществом, используемым в целях предпринимательской деятельности, либо если эти преступления совершены членом органа управления коммерческой организации в связи с осуществлением им полномочий по управлению организацией при выполнении коммерческой организацией предпринимательской или иной экономической деятельности.

На данной стадии проверки сообщения о преступлении лицо, как правило, не установлено. Для этого органом дознания проводятся оперативно-розыскные мероприятия, указанные в ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». В ст. 7–8 Федерального закона «Об оперативно-розыскной деятельности» определены основания и условия проведения оперативно-розыскных мероприятий. К ним относятся наличие возбужденного уголовного дела; ставшие известными сведения о признаках преступления совершенного, планируемого в будущем, совершаемого в настоящее время, о лицах, его совершивших или совершаемых, подготавливающих, если недостаточно собранных данных для возбуждения уголовного дела.

Проведение оперативно-розыскных мероприятий, ограничивающих конституционные права граждан на тайну переписки, право на неприкосновенность жилища, допустимы только при наличии судебного решения и информации о подготавливаемом, совершаемом или совершенном преступлении, по которому предварительное следствие обязательно [5]. Результаты оперативно-розыскных мероприятий, связанных с ограничением конституционных прав граждан, могут быть использованы как доказательства лишь в том случае, если они получены по решению суда на проведение оперативно-розыскных мероприятий и проверены следственными органами в соответствии с УПК РФ [5].

Таким образом, согласно ст. 150 «Формы предварительного расследования» УПК РФ, по ч. 1 ст. 159.6УК РФ производится дознание, что, в свою очередь, исключает из перечня оперативно-розыскных мероприятий такие, которые связаны с ограничением конституционных прав: «обследование помещений, зданий, сооружений, участков местности и транспортных средств», «контроль почтовых отправлений, телеграфных и иных сообщений», «прослушивание телефонных переговоров», «получение компьютерной информации» [6].

На первоначальном этапе расследования компьютерных преступлений, в том числе при осуществлении доследственной проверки, необходимо собрать как можно больше сведений о преступлении. Следует получить первичную информацию о времени преступления, для поиска «следов» инструментария и ответов на вопросы по предмету доказывания: «Что? Где? Когда? Кто? Каким способом? Зачем? Почему?». Первичная информация способствует правильному выдвижению криминалистических версий, планированию и эффективному производству неотложных следственных действий. Данные об объективной стороне исследуемых преступлений в основном находятся в «виртуальном» пространстве. В связи с этим для получения оперативно значимой информации необходимо провести осмотр места преступления и средств компьютерной техники. При расследовании обычно существует информация хотя бы об одном устройстве с электронно-цифровыми следами преступления, как правило, речь идет об устройстве потерпевшего. При осуществлении неотложных следственных действий, например, осмотра места преступления и компьютерной техники,

важно прежде всего провести фиксацию криминалистически значимой компьютерной информации, которая может быть безвозвратно потеряна. Зачастую она может быть обнаружена в энергозависимой части устройств, например, в оперативной памяти. После этого можно зафиксировать компьютерную информацию, хранящуюся в энергонезависимой части устройств.

После фиксации информации можно ее проанализировать и оценить. Особое внимание должно быть уделено поиску негативных обстоятельств, то есть нехарактерным признакам, имеющимся в «виртуальной» обстановке преступления, если отсутствуют следы, которые по характеру обстоятельств должны быть или, наоборот, присутствуют такие следы, которых не должно быть. Так, в одном из защищенных лог-файлов сохранилась запись об операции копирования на флеш-память, а в основных лог-файлах записи о подключении каких-либо устройств к компьютеру не содержится. В высокотехнологичных способах совершения преступлений поиск таких негативных обстоятельств порой является единственной возможностью раскрытия преступления.

При обнаружении негативных обстоятельств неотложно проводят обыск, затем его нужно санкционировать в связи с вероятностью уничтожения и сокрытия следов преступления, совершаемых опытными преступниками. Во время обыска или экспертизы можно осуществить восстановление удаленных файлов за интересующий период. Восстановление всех файлов без учета предварительного промежутка времени, в период которого совершено преступление, изменит информацию, отображаемую в информационной обстановке в интересующий нас период, и приведет к искажению информации, а впоследствии – к неправильно построенным версиям.

В ситуации обнаружения негативных обстоятельств следствию целесообразно, применив ретроспективную методику, попытаться максимально восстановить картину происшествия: информационную обстановку преступления до и после применения мер сокрытия следов преступления. Для этого, в частности, можно построить список запущенных приложений в хронологическом порядке, отразив запросы к интернет-ресурсам (через историю браузера), построить список IP-адресов с портами по коммуникации.

На данном этапе могут быть выделены ситуации, когда средства удаленного совершения преступлений подразделены по виду собственности; мобильности средств совершения преступлений; характеру построения канала связи; энергозависимой части компьютерной информации. IP-адрес имеет свой ресурс нумерации, то есть каждому интернет-провайдеру выделено определенное количество IP-адресов в конкретном диапазоне. При помощи интернет-ресурса *www.2ip.ru* (прямая ссылка *www.2ip.ru/whois/*), зная IP-адрес, можно легко определить провайдера. Установив IP-адрес и точное время его использования в сети Интернет, можно узнать адрес нахождения персонального компьютера, с которого работал преступник (адрес квартиры, частного дома или кафе).

Следует отметить, что существуют статические и динамические IP-адреса. Динамические IP-адреса предоставляют операторы сотовой связи для интернет-сессии с использованием модемов 3*G*, 4*G* мобильных устройств (смартфонов, планшетов), а также для доступа к банковским сервисам через мобильные приложения. В таких случаях в запросе интернет-провайдерам, операторам сотовой связи необходимо указывать максимально имеющиеся сведения о дате, времени, использованных динамических IP-адресах, а также IP-адресах ресурса обращения, то есть внешний IP-адрес интернет-сайта. Сведения о внешнем IP-адресе необходимо запросить у администратора интернет-сайта, который посещал злоумышленник.

Установление местонахождения преступника по IP-адресам усложняет использование им легкодоступных средств анонимизации в сети: *Virtual Private Network*, *VPN* (виртуальная частная сеть) и *Proxy*. Суть виртуальной частной сети заключается в том, что пользователь ин-

тернета, прежде чем выйти на сайт, подключается к серверу третьего лица, как правило, локализующегося на территории иного государства. Запрос на интернет-сайт проходит аналогично, как описано ранее. Однако в истории соединений сайта остается не IP-адрес пользователя, а IP-адрес использованного им *VPN*-сервера.

Установив компанию, обслуживающую *VPN* или *Proxy*-сервер, необходимо запросить данные об IP-адресе пользователя, указав максимальную имеющуюся информацию о временных промежутках выхода в интернет и IP-адреса интернет-ресурсов, к которым осуществлялось обращение. Большое количество *VPN* и *Proxy*-серверов принадлежит иностранным интернет-провайдерам, в адрес которых возможно направить запрос через Интерпол, по международным запросам, в рамках расследования уголовных дел.

Построение ситуации, вытекающей из сочетания результатов по предложенным классификациям, позволяет лучшим образом очертить возможный механизм преступления. Эти данные необходимы для построения корреляционных зависимостей с другими элементами криминалистической характеристики преступлений, которые следует установить.

Речь идет о «построении информационной обстановки» устройства в промежуток времени предполагаемого преступления (до и после применения мер сокрытия следов преступления), то есть построение списка запущенных приложений и их очередность, запросы к интернет-ресурсам (через историю браузера); построении списка IP-адресов с портами по коммуникации за интересующийся промежуток времени с *Log*-файлов. Для формирования объективной картины произошедших событий целесообразно исследовать информацию, находящуюся на устройствах, участвующих в передаче информации по телекоммуникационной сети связи. К таким устройствам относятся маршрутизаторы провайдера, прокси-сервера, конечные удаленные сервера, обеспечивающие работу приложений и т.д.

Далее необходимо снова проанализировать и оценить информационную обстановку, но, сопоставив данные на обнаруженной компьютерной технике с его сетевым трафиком, полученным от провайдера. Полученные данные должны быть выстроены в хронологическом порядке: о запущенных приложениях, запросах к интернет-ресурсам, построении маршрутов внешнего IP-адреса устройства с IP-адресами по трафику, предоставленному провайдером, сопоставлении информации по семи уровневой модели *OSI* (физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной уровни). Далее – построение информационной обстановки в хронологическом порядке информации на устройстве в соответствии с разложенным по семи уровневой модели *OSI* трафиком устройства. В результате может быть обнаружена криминалистически значимая информация (о признаках использования удаленного доступа, виртуальной машины, IP-телефонии, шифрования данных; использования *VPN*, шифрации трафика, использования выделенного сервера «дедика», прокси-анонимайзера), которая может свидетельствовать о сокрытии следов преступления и участия в нем, а также указывать на высокотехнологичный способ совершения преступления.

Отработка версий – это анализ полученных ответов от интернет-ресурсов (расположенных в России), провайдеров, исследование компьютерной техники и устройств, которые имели соединения с внешним IP-адресом устройства потерпевшего. По версиям происходит сопоставление компьютерной информации, снятой с устройства потерпевшего, с информацией, полученной при проведенных оперативно-розыскных мероприятиях. Иными словами, необходимо установить, подтверждается ли ранее выдвинутая версия о механизме преступления (по классификации) либо отвергается. Если версия подтверждается, то отправляется запрос информации по всем посредникам построения канала связи для фиксации значимой компьютерной информации, для последующего установления устройства связи «злоумышленника». Если версия

отвергается, то проводится анализ следующей версии или построение новой на основе полученной информации.

ЛИТЕРАТУРА

1. Аналитический обзор опыта работы органов предварительного следствия по уголовным делам о преступлениях, совершенных в сфере информационно-телекоммуникационных технологий, по итогам 2020 года // Письмо Следственного департамента МВД России от 4 июня 2021 г.

2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18 декабря 2001 г.(в ред. от 11 июня 2022 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 18.06.2022).

3. Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63-ФЗ (в ред. от 11 июня 2022 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 18.06.2022).

4. Определение Конституционного Суда РФ от 16 июля 2013 г. № 1156-О // Гарант.ру: информационно-правовой портал. URL: https://base.garant.ru/70455018/ (дата обращения: 18.06.2022).

5. Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 // Верховный Суд РФ. URL: http://www.vsrf.ru/documents/own/8342/ (дата обращения: 18.06.2022).

6. Об оперативно-розыскной деятельности: федер. закон от 12 августа 1995 г. № 144 // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 18.06.2022).