**УДК** 343.98
**DOI:** 10.19073/2658-7602-2026-23-2-305-318
**EDN:** CCOAXC



*Оригинальная научная статья*

# Роль межведомственного взаимодействия в выявлении преступников, анонимизирующих свою личность

**Д. В. Воробьева**
*Уральский юридический институт МВД России, Екатеринбург, Российская Федерация*
✉ *dacha_vorobyeva_13@mail.ru*

**Аннотация.** В статье предпринята попытка рассмотрения возможностей взаимодействия при установлении личности преступника в сети Интернет в ходе расследования компьютерных преступлений. В связи с ростом числа нераскрытых преступлений в сфере компьютерной информации вследствие использования преступниками средств анонимизации, а также недостаточного уровня специальных знаний сотрудников правоохранительных органов в сфере информационных технологий представляется необходимым рассмотреть возможности раскрытия данных категорий преступлений посредством координации действий с другими структурными подразделениями и организациями. Предметом настоящего исследования являются закономерности получения (сбора) идентификационных данных о личности преступника при осуществлении взаимодействия с операторами сотовой связи, провайдерами, оперативными сотрудниками, специалистами и т. д. Цель данного исследования заключается в выявлении и решении проблем установления личности преступника, анонимизирующего свою личность, а также в рассмотрении отдельных форм взаимодействия, позволяющих решить указанную проблему. В основу исследования положен междисциплинарный подход и общенаучные методы познания (анализ, синтез, системно-структурный метод, описание). Делается вывод о том, что с учетом складывающейся негативной практики расследования указанных категорий преступлений преодоление данных видов противодействия возможно посредством комплексного взаимодействия с рассмотренными в статье структурными подразделениями и органами в целях эффективного выявления и установления личности преступника. Разделение функций (операторы сотовой связи – сбор базовых данных абонентов и геолокации; провайдеры – логирование трафика; социальные сети – доступ к метаданным и контенту; оперативные сотрудники – постоянный мониторинг открытых источников и взаимодействие с другими подразделениями; специалисты – анализ следов, участие в следственных действиях и консультирование) минимизирует временные потери, уменьшит вероятность ошибок и допущения тактических рисков. При гармоничном и законном взаимодействии вышеуказанных участников вероятность корректной идентификации личности преступника в сети Интернет значительно возрастает. Такой подход обеспечивает не только задержание злоумышленника и блокировку используемых им информационных ресурсов, но и получение надежной доказательственной базы, минимизируя риски нарушения прав граждан.

**Ключевые слова:** взаимодействие; ведомственные органы; вневедомственные организации; предоставление информации; деанонимизация; идентификационные данные

**Конфликт интересов.** Автор заявляет об отсутствии конфликта интересов.

**Для цитирования:** Воробьева Д. В. Роль межведомственного взаимодействия в выявлении преступников, анонимизирующих свою личность // Сибирское юридическое обозрение. 2026. Т. 23, № 2. С. 305–318. DOI: https://doi.org/10.19073/2658-7602-2026-23-2-305-318. EDN: https://elibrary.ru/ccoaxc

*Original scientific article*

# The Role of Interagency Cooperation in Identifying Offenders Who Anonymize Their Identity

**D. V. Vorobyeva**

*Ural Law Institute of the Ministry of the Interior of Russia, Yekaterinburg, Russian Federation*

✉ *dacha_vorobyeva_13@mail.ru*

**Abstract.** This article attempts to examine the possibilities of cooperation in establishing the identity of an offender on the Internet during the investigation of computer crimes. In view of the growing number of unsolved crimes in the field of computer information, caused by offenders' use of anonymization tools, as well as by the insufficient level of specialized knowledge in information technology among law-enforcement officers, it is necessary to consider the possibility of detecting and solving such crimes through the coordination of actions with other structural units and organizations. The subject of this study is the patterns involved in obtaining and collecting identification data concerning an offender's identity through cooperation with mobile network operators, Internet service providers, operational officers, specialists, and other relevant actors. The aim of the study is to identify and address the problems involved in establishing the identity of an offender who anonymizes his or her identity, and to examine particular forms of cooperation that may help resolve this problem. The study is based on an interdisciplinary approach and general scientific methods of cognition, including analysis, synthesis, the systemic-structural method, and description. The article concludes that, given the emerging negative practice in the investigation of this category of crimes, these forms of counteraction can be overcome through comprehensive cooperation with the structural units and bodies discussed in the article, with a view to effectively detecting the offender and establishing his or her identity. The division of functions — mobile network operators collecting basic subscriber and geolocation data; Internet service providers logging traffic; social networks providing access to metadata and content; operational officers continuously monitoring open sources and interacting with other units; and specialists analyzing traces, participating in investigative actions, and providing advice — minimizes time losses, reduces the likelihood of errors, and lowers tactical risks. Where the above-mentioned participants interact in a coordinated and lawful manner, the probability of correctly identifying an offender on the Internet increases significantly. This approach ensures not only the detention of the offender and the blocking of the information resources used by him or her, but also the collection of a reliable evidentiary basis, while minimizing the risk of violating citizens' rights.

**Keywords:** cooperation; departmental bodies; non-departmental organizations; provision of information; deanonymization; identification data

**Conflict of interest.** The Author declares no conflict of interest.

**For citation:** Vorobyeva D. V. The Role of Interagency Cooperation in Identifying Offenders Who Anonymize Their Identity. *Siberian Law Review.* 2026;23(2):305-318. DOI: https://doi.org/10.19073/2658-7602-2026-23-2-305-318. EDN: https://elibrary.ru/ccoaxc (In Russ.)

## Содержание

## I. Введение

В условиях глобальной цифровизации общества сеть Интернет стала не просто средством коммуникации, обмена и поиска информации, обучения и трудовой деятельности, но и благоприятной средой для осуществления преступной деятельности. Данный феномен обусловлен тем, что глобальная сеть со временем преобразовалась в массивное хранилище колоссального объема информации, в котором можно найти разнообразные сведения – от персональных данных человека до алгоритмов по совершению преступлений. Но информационное обеспечение преступности не является единственной проблемой влияния Интернета на рост преступной активности в цифровом сегменте. Одновременно модернизируются способы совершения преступлений, приобретая дистанционный характер, который влечет за собой трансграничность преступности, меняется следовая картина преступного события, что приводит к изменениям способов сокрытия преступления. Все эти факторы неизбежно сказываются на раскрытии и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – IT-технологии) и в сфере компьютерной информации.

Несмотря на большое количество преступлений, совершаемых с использованием IT-технологий и в сфере компьютерной информации, наибольший интерес для нашего исследования представляет неправомерный доступ к компьютерной информации (ст. 272 Уголовного кодекса Российской Федерации). Интерес к данной категории преступлений вызван существующим в ее структуре феноменом анонимизации личности преступника, обусловливающим низкую раскрываемость этого вида преступлений. Использование анонимизирующих средств и методов позволяет преступнику скрывать идентификационные данные своей личности, что затрудняет процесс его изобличения.

Большинство существующих научных работ, которые посвящены исследованию феномена анонимизации, относятся к области информационной безопасности и других компьютерно-технических наук [1; 2; 3; 4]. Однако распространенное использование данных средств в преступной деятельности позволяет говорить о необходимости рассмотрения этого явления криминалистической наукой, а также о разработке мер по противодействию ему.

Следует отметить, что в условиях цифровизации преступности правоохранительным органам становится сложнее бороться с ней изолированно, в связи с чем они осуществляют взаимодействие с другими структурными подразделениями, органами и организациями для увеличения объема сил и средств в целях преодоления противодействия.

В рамках настоящей статьи представляется необходимым более подробно исследовать возможности взаимодействия в ходе установления преступников, анонимизирующих свою личность при совершении неправомерного доступа к компьютерной информации.

В основу методологии исследования положены общенаучные методы познания (анализ, синтез, системно-структурный метод, описание), а также междисциплинарный подход, позволивший объединить юридические криминалистические знания со сферой изучения современных компьютерных технологий.

## II. Проблемы деанонимизации личности преступника

Сложность расследования данной категории преступлений обусловлена тем, что преступники предпринимают меры по сокрытию информации о себе еще при подготовке к совершению преступления, что приводит к возникновению

проблемных следственных ситуаций на первоначальных этапах расследования, обусловленных информационной недостаточностью данных о лице, совершившем преступление.

Проблема установления личности преступника на сегодняшний день стоит достаточно остро. Вопросами деанонимизации лиц, совершающих преступления в сети Интернет занимались С. В. Тимофеев [5], А. И. Гайдин [6], Ю. В. Гаврилин [7], С. И. Земцова [8] и др. В своих работах они рассматривали организационно-тактические проблемы, проблемы правового регулирования деятельности оперативных подразделений по получению информации из сети Интернет, проблемы материально-технического и организационно-управленческого характера.

Анализ практической деятельности правоохранительных органов и научной литературы по данному направлению показал, что факторы, оказывающие негативное влияние на достижение результатов по установлению личности преступника в сети Интернет, можно разделить на субъективные и объективные.

К субъективным факторам следует относить:

– отсутствие достаточного опыта в раскрытии и расследовании неправомерного доступа к компьютерной информации [5, с. 113];

– отсутствие соответствующих знаний в области информационных технологий, веб-разработки и сетевой безопасности;

– стереотипные представления о сложности расследования данных преступлений и неуверенность в себе и своих силах;

– неграмотная работа с цифровыми следами.

Объективные факторы:

– использование преступниками высокотехнологичных средств анонимизации;

– трансграничный характер преступлений данных видов;

– отсутствие методических рекомендаций по раскрытию и расследованию данных преступлений;

– недостаточное количество сил и средств, позволяющих в короткие сроки выявлять и устанавливать необходимую информацию, имеющую значение для уголовного дела.

Среди перечисленных факторов, оказывающих негативное влияние на раскрытие неправомерного доступа к компьютерной информации, одним из главных, на наш взгляд, выступает использование в ходе совершения преступления средств анонимизации, позволяющих преступнику скрывать идентификационные данные о своей личности. Названный фактор оказывает влияние как на установление данных о лице, так и на раскрытие и расследование преступления в целом.

Отметим, что на первоначальных этапах расследования главная задача правоохранительных органов заключается в обнаружении следов, позволяющих установить личность преступника. К таким следам относятся:

1) IP-адрес устройства, используемого преступником при совершении преступления рассматриваемого вида, а также при его сокрытии;

2) MAC-адрес – идентификатор устройства, используемого для доступа к сети Интернет (например, роутера);

3) IMEI – уникальный номер, например мобильного устройства (средства связи);

4) следы используемого интернет-провайдера – организации, обеспечивающей услуги по подключению к сети Интернет в определенном месте (месте преступления);

5) ID-пользователя в социальной сети – уникальный номер, присваиваемый пользователю учетной записи;

6) username – это уникальное имя пользователя, которое идентифицирует аккаунт на платформе социальной сети;

7) номер телефона;

8) адрес электронной почты;

9) данные браузера, операционной системы и т. д.

В условиях анонимизации личности преступника установление указанных идентификаторов следователем самостоятельно в рамках производства осмотра технического устройства потерпевшего или допроса потерпевшего не представляется возможным, вследствие чего следователи прибегают к помощи сотрудников других ведомств или структур, обладающих наибольшим объемом специальных знаний и средств, позволяющими получить необходимые данные.

Для исследования данного вопроса представляется необходимым более подробно рассмотреть возможности взаимодействия и роль, которую оно играет в установлении идентификационных данных о личности преступника, использующего средства анонимизации.

В криминалистической литературе под взаимодействием принято понимать согласованную деятельность различных звеньев одной или нескольких организованных систем, направленную на достижение общей цели с наименьшими затратами сил, средств и времени.

Вопросам организации взаимодействия участников расследования преступлений посвящены работы А. В. Гордина[1], Н. А. Аменицкой[2], И. А. Данилкина [9], Т. А. Паутовой[3], В. И. Пархоменко[4], а также ряда других ученых. В своих трудах они рассматривали особенности взаимодействия органов предварительного следствия с органами дознания, исследовали формы такого взаимодействия и их нормативно-правовое регулирование.

В рамках настоящей работы мы не будем ограничиваться рассмотрением вопросов взаимодействия лишь с органами дознания, а рассмотрим данный вопрос с точки зрения организации взаимодействия с ведомственными структурными подразделениями и вневедомственными организациями.

## III. Взаимодействие с вневедомственными организациями

Ввиду многообразия способов совершения неправомерного доступа к компьютерной информации, преступники используют различные средства как для совершения преступления, так и для его сокрытия, при этом оставляя за собой следы. Обнаружение таких следов, их фиксация, изъятие и исследование требуют вовлечения в процесс расследования значительного числа субъектов – представителей правоохранительных и иных государственных органов, коммерческих организаций, осуществляющих деятельность в сфере предоставления информационных, коммуникационных и финансовых услуг.

Например, М., используя приобретенный им мобильный телефон *Redmi Note 9 Pro* и сим-карту оператора ПАО «Мегафон», реализуя свой преступный умысел, направленный на получение персональных данных для входа в личный кабинет «СбербанкОнлайн», принадлежащий К., осуществил преступный сговор с Н.,

[1] См.: *Гордин А. В.* Взаимодействие оперативно-розыскных служб и следователя органов внутренних дел при расследовании преступлений : дис. … канд. юрид. наук. СПб., 2005. 208 с.

[2] См.: *Аменицкая Н. А.* Взаимодействие следователя и органов, осуществляющих оперативно-розыскную деятельность в раскрытии и расследовании преступлений (в ОВД) : дис. … канд. юрид. наук. Н. Новгород, 2006. 201 с.

[3] См.: *Паутова Т. А.* Взаимодействие следователей органов внутренних дел с органами дознания при возбуждении и расследовании уголовных дел : дис. … канд. юрид. наук. Тюмень, 2005. 183 с.

[4] См.: *Пархоменко В. И.* Взаимодействие следователей, оперативных работников и специалистов при расследовании уголовных дел о незаконном обороте наркотических средств и психотропных веществ (тактико-криминалистический и организационный аспекты) : дис. … канд. юрид. наук. М., 2005. 230 с.

имеющим водительское удостоверение, с целью сокрытия следов преступления путем смены точек положения базовых станций при передвижении на автомобиле, принадлежащем Н., в ходе осуществления звонков К. Так, М., передвигаясь на автомобиле под управлением Н., осуществил звонок потерпевшей К., имитируя женский голос, сообщил ложные сведения о том, что он является сотрудником ПАО «Сбербанк», а также о том, что у нее якобы накопились бонусы по программе «СберСпасибо», которые она может получить. В ходе телефонного разговора М. убедил К. сообщить ему номер банковской карты и код подтверждения, необходимые для доступа к личному кабинету мобильного приложения «СбербанкОнлайн». После чего М. совершил вход в личный кабинет и получил доступ к денежным средствам, принадлежащим К.[5]

Исходя из приведенного примера, следует отметить, что установлению будут подлежать следующие идентификационные данные: IMEI телефона злоумышленника, номер телефона, сведения об адресе базовой станции, IP-адрес и т. д. Это свидетельствует о необходимости обращения в организации, обладающие соответствующей информацией. Установление указанных сведений и других идентификационных данных, происходит посредством взаимодействия с такими субъектами, как операторы сотовой связи, банковские организации, администраторы социальных сетей, интернет-провайдеры.

Организация взаимодействия с данными субъектами осуществляется путем направления в их адрес запросов с просьбой предоставить интересующую органы внутренних дел информацию.

Анализ судебной практики и материалов уголовных дел показывает, что при направлении запросов операторам сотовой связи следователи допускают ошибки, связанные с тем, что запрашивают у операторов детализацию входящих и исходящих соединений по абонентскому номеру, забывая запросить адреса базовых станций, обеспечивающих телефонную связь пользователей, а также данные об IMEI, которые в совокупности свидетельствуют о принадлежности телефона конкретному физическому лицу и позволяют оперативно получить необходимую информацию, сократив сроки расследования. Также ошибки допускаются при направлении запросов администраторам социальных сетей: следователи могут ограничиться лишь получением данных об IP-адресе и номере телефона, указанном при регистрации аккаунта, забывая истребовать данные о фамилии, имени и отчестве пользователя, которые могут не совпадать с указанным никнеймом, о времени входа в социальную сеть и выхода из нее и т. д. Перечисленные сведения выступают отправной точкой в цепочке следов, позволяющих установить участников преступления и пострадавших, поэтому промедление в предоставлении такой информации значительно затягивает процесс расследования и оказывает негативное влияние на доказывание отдельных обстоятельств [10, с. 153].

Таким образом, с учетом сложностей, возникающих при составлении запросов в процессе организации взаимодействия с коммерческими организациями, представляется целесообразным привести перечень информации, необходимой для расследования неправомерного доступа к компьютерной информации.

В случаях, когда у правоохранительных органов имеется информация об абонентском номере, следователь может получить у *оператора сотовой связи* следующие данные:

[5] См.: *Приговор* Кировск. Район. суда г. Волгограда от 16 марта 2025 г. № 1-100/2025 по делу № 1-100/2025 // Судеб. и норматив. акты РФ. 2025. URL: https://sudact.ru/regular/doc/eMepwe9YubH0/ (дата обращения: 06.01.2026).

– паспортные данные владельца абонентского номера;

– детализацию звонков[6];

– IMEI устройств, с которых осуществлялась связь в течение последних трех месяцев;

– сведения о базовых станциях, через которые осуществлялась связь;

– информацию о входящих и исходящих платежах по лицевому счету, связанному с данным абонентским номером;

– информацию об IP-адресах, использованных для входа в личный кабинет абонента у сотового оператора и управления данным номером[7].

Информация, предоставленная оператором сотовой связи, может носить как доказательственный, так и ориентирующий характер [11, с. 187]. Представленная информация позволяет получить сведения об используемом интересующим лицом оборудовании (средствах связи), выявить круг лиц активного общения, в том числе возможных соучастников преступных действий (в процессе анализа протоколов соединений, осуществлявшихся с используемых абонентских номеров) и установить местонахождение конкретного лица (телефона с абонентским номером) в определенное время[8].

В случаях совершения преступления с использованием социальных сетей правоохранительные органы при взаимодействии с *администраторами социальной сети* могут получить следующую информацию:

– установочные данные, использованные лицом для регистрации (абонентский номер и (или) адрес электронной почты);

– IP-адрес, используемый для создания и доступа к странице;

– периоды посещения сайта;

– сведения о смене логина и пароля;

– сведения о смене никнейма;

– сведения о времени пребывания пользователя на сайте, просмотренном и скачанном контенте, а также об используемом браузере;

– данные об идентификаторе (ID) пользователя в социальной сети.

Среди всей представленной информации наибольшую ценность имеют сведения об IP-адресе. IP-адрес присваивается вычислительному устройству клиента (пользователя) интернет-провайдером [12, с. 85]. Сотрудники, направив запрос *интернет-провайдеру*, могут получить следующую дополнительную информацию о пользователе:

– полные данные, указанные лицом при заключении договора об оказании интернет-услуг (фамилию, имя, отчество, адрес, номер телефона, копию паспорта);

– адрес местонахождения приемопередающего оборудования, посредством которого осуществлялся выход в сеть Интернет через указанный IP-адрес;

– информацию о том, является ли данный IP-адрес статическим или динамическим;

– информацию об используемом 3G- или 4G-модеме (номер SIM-карты, MAC-адрес), посредством которого осуществлялся выход в сеть Интернет через указанный IP-адрес [13].

Еще одним источником получения криминалистически значимой информации являются отправления электронной почты и соответствующие интернет-сервисы по предоставлению подобных услуг. Это не только информация, содержащаяся в тексте самого почтового отправления,

[6] Указанные сведения позволяют определить входящие и исходящие звонки данного абонента за необходимый период времени, номера телефонов абонентов, с которыми происходили соединения, продолжительность соединений, а также дополнительно можно получить информацию о базовой станции с указанием их направленности и секторов.

[7] Следует отметить, что получение данной информации осуществляется на основании судебного решения, поскольку указанные данные, в соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи», являются информацией ограниченного доступа.

[8] См.: *Козинкин В. А.* Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи : автореф. дис. … канд. юрид. наук. М., 2009. С. 11–12.

но и информация о маршруте его следования в процессе отправки-получения (RFC-заголовок, служебный заголовок, свойства письма, для ознакомления с которыми необходимо открыть электронное письмо и в командной панели выбрать команду отображения свойств письма). Данная информация содержит сведения об IP-адресе, с которого письмо было отправлено, и фактический адрес электронной почты отправителя. Как правило, IP-адрес отправителя содержится в строках *X-Originating-IP* или *Received: from* свойств электронного почтового отправления[9].

К криминалистически значимой информации, которую возможно получить в организациях, являющихся *собственниками интернет-сервисов электронной почты,* относятся сведения, содержащиеся в учетной записи (аналогично социальным сетям), данные о сеансах доступа к электронному почтовому ящику, сведения о произведенных в учетной записи изменениях (смена пароля, номера телефона, контрольного вопроса и т. п.), переписка пользователя (по судебному решению).

Помимо текстовых сообщений через электронную почту потерпевшему могут быть направлены сообщения, содержащие ссылки на фишинговые сайты, в адресной строке которых отображается доменное имя сайта.

В адрес сайтов, осуществляющих регистрацию доменных имен, направляется запрос о предоставлении следующей информации:

– о паспортных данных регистратора доменного имени;

– абонентских номерах и адресах электронной почты, использованных при регистрации;

– IP-адресах, использованных для регистрации доменного имени;

– IP-адресах, использованных для входа в личный кабинет или для доступа к панели управления для администрирования доменного имени;

– оплате услуг регистрации и аренды доменного имени с указанием полных реквизитов плательщика.

Как правило, ввиду отсутствия очевидцев совершения неправомерного доступа к компьютерной информации и взаимодействия преступника с потерпевшим через информационно-телекоммуникационную сеть налаживание взаимодействия с указанными организациями становится критически важным [14, с. 16]. Так, Ю. В. Гаврилин отмечает, что повышению эффективности внешнего взаимодействия способствует использование территориальными органами внутренних дел системы электронного документооборота, а также заключение соглашений об информационном обмене с кредитно-финансовыми организациями и организациями связи [15, с. 146]. Это также имеет немаловажное значение для сокращения сроков получения необходимой информации при раскрытии и расследовании преступлений. На сегодняшний день такие соглашения заключены лишь с банковскими организациями ПАО «Сбербанк России», АО «КИВИ Банк»[10], а также оператором сотовой связи ПАО «Мегафон», что, на наш взгляд, требует расширения перечня организаций.

## IV. Взаимодействие с ведомственными субъектами

В процессе расследования преступлений в сфере компьютерной информации следователи используют всевозможные процессуальные и непроцессуальные формы взаимодействия с сотрудниками правоохранительных органов. Наиболее

[9] См.: *Деятельность* органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учеб.пособие : в 2 ч. / Ю. В. Гаврилин, А. В. Аносов, В. В. Баранов, Н. П. Голяндин [и др.]. М. : Акад. управления МВД России, 2019. Ч. 1. С. 115.

[10] По данным Центрального банка Российской Федерации, АО «Киви Банк» ликвидирован с 22 декабря 2025 г. .

тесное взаимодействие на всех этапах расследования осуществляется с оперативными сотрудниками подразделений органов внутренних дел [16, с. 179].

В зависимости от складывающейся следственной ситуации и категории дел следственные органы осуществляют выбор одной из двух форм взаимодействия либо используют их в совокупности.

По мнению С. С. Босхолова, И. С. Брагиной и С. Н. Серикова, «наибольший успех при раскрытии и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, достигается при активном оперативно-розыскном сопровождении, суть которого заключается в комплексном использовании современных программно-аппаратных комплексов и методов оперативно-розыскной деятельности, направленных на изобличение и документирование противоправной деятельности лица, совершившего преступление» [17, с. 73]. Разделяя данную точку зрения, полагаем, что в рассматриваемом нами вопросе установление личности преступника невозможно без помощи сотрудников оперативных подразделений, поскольку в их ведении находится больше средств, которые расширяют границы поиска и экономят время.

В 2022 году, согласно Указу Президента Российской Федерации, в структуре центрального аппарата МВД России было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (далее – УБК)[11]. УКБ реализует функции по борьбе с преступлениями в сфере компьютерной информации, совершенными с использованием IT-технологий, а также противодействует распространению противоправной информации в сети Интернет.

В ходе раскрытия и расследования неправомерного доступа к компьютерной информации следственные органы осуществляют взаимодействие с оперативным подразделением УКБ. Эффективность данного взаимодействия обусловлена тем, что оперативные сотрудники УБК обладают более глубокими специальными знаниями и навыками поиска и обнаружения личности преступника ввиду их узкой специализации.

Среди форм процессуального взаимодействия на первоначальных этапах расследования можно выделить исполнение поручений по установлению лица, совершившего преступления. Однако, к сожалению, и в данном направлении практика складывается не всегда благоприятно. Связано это с тем, что сотрудники органа дознания формально подходят к исполнению поручений следователя по установлению личности преступника. При выполнении поручений поисковые мероприятия прекращаются на этапе получения сотрудниками информации о подменном IP-адресе, при этом игнорируются возможности установления лица по иным идентификаторам. Данная негативная тенденция может быть обусловлена отсутствием знаний об иных методах установления личности преступника.

Речь идет об использовании сотрудниками оперативных подразделений методов *OSINT*[12] при установлении личности

[11] См.: *О внесении* изменений в некоторые акты Президента Российской Федерации : Указ Президента Рос. Федерации от 30 сент. 2022 г. № 688. Доступ из СПС «КонсультантПлюс».

[12] *OSINT* (англ. *Open Source Intelligence* – «разведка по открытым источникам») – это разведывательная деятельность, включающая в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ. В качестве открытых источников могут быть использованы средства массовой информации (новостные статьи и телевизионные документальные фильмы), интернет-издания, сообщества, форумы, видеохостинги, социальные сети, отчеты аналитических центров, а также результаты социальных опросов, статистические данные, судебная практика, открытые базы данных (реестры, база знаний MITRE ATT&CK), научные работы.

преступника. Согласно результатам анкетирования, проведенного среди сотрудников оперативных подразделений, следствия и дознания, 73,4 % респондентов не используют методы *OSINT* при установлении личности преступника.

В настоящее время указанная форма получения данных об искомом лице является достаточно результативным способом.

Так, если преступник получил неправомерный доступ к компьютерной информации, используя в ходе совершения преступления социальные сети, но при этом с помощью VPN-сервиса скрыл свой IP-адрес, то сведения о его личности могут быть получены посредством его никнейма. Первым шагом является установление идентификатора, по которому можно обнаружить профиль. В данном случае им является никнейм, но, помимо него, могут быть обнаружены и использованы номер телефона, адрес электронной почты, адреса криптовалютных кошельков, индивидуальный идентификатор (ID) и т. п.

Сотруднику необходимо проверить наличие профилей фигуранта на всех популярных платформах и сервисах:

– социальных сетях (Facebook[13], «ВКонтакте», «Одноклассники», Instagram[14], LinkedIn, X (Twitter), «Дзен»);

– мессенджерах (Telegram, WhatsApp, Viber, Discord, «Макс» и др.);

– сервисах электронной почты (Gmail, Mail.ru, «Яндекс Почта», «Рамблер/почта»);

– маркетплейсах (OZON, Wildberries, Lamoda, «Яндекс Такси», «Яндекс Еда», «Деливери», Uber, «Самокат», «Купер»);

– форумах и имиджбордах (Reddit, 4chan, 2ch, «Хабр»);

– сайтах объявлений («Авито», «Юла» и др.);

– геосоциальных сервисах («Яндекс Карты», Google Maps и др.);

– хостингах изображений и видео (YouTube, TikTok, Likee, RuTube);

– игровых платформах (Steam, PlayStation Store, Network Gaming);

– криптовалютных биржах и обменниках (Binance, Coinbase).

Важно отметить, что анализу подлежат не только популярные платформы, но и нишевые, специфические сайты. Часто именно на малоизвестных ресурсах пользователи ведут себя менее осторожно и оставляют сведения, имеющие значение для их деанонимизации.

Установление связи между аккаунтами происходит посредством выявления совпадений по различным идентификационным признакам: схожие или производные имена пользователей, никнеймы, псевдонимы (например, Vanya_Ivanov, VanyaIvanov1987, IvanovVanya, IvanovV_1987 и т. п.); одинаковые адреса электронной почты и (или) номера телефонов, повторяющиеся или сходные по стилю аватары профилей, фотографии, изображения в постах, схожие стили письма, синхронность публикаций, совпадения по времени активности и т. д.

Методы *OSINT* могут применяться и для получения вышеуказанных идентификационных данных с целью экономии времени при получении ответов на запросы от операторов сотовой связи, банковских организаций и т. д. Информация, полученная с использованием методов *OSINT*, имеет важное значение для эффективного раскрытия преступления, выдвижения версий, возбуждения уголовного дела, грамотного применения тактических приемов при производстве следственных действий, планирования и организации подготовки проведения тактических операций (комбинаций), следственных действий, а также правильного выстраивания алгоритма действий на различных этапах расследования по уголовному делу [18, с. 64].

[13] Признана экстремистской организацией и запрещена на территории Российской Федерации.
[14] Признана экстремистской организацией и запрещена на территории Российской Федерации.

Помимо рассмотренной формы взаимодействия, оперативное сопровождение может осуществляться при проведении отдельных следственных действий, реализации тактических операций по установлению и задержанию искомого лица, а также в случаях оказания содействия в рамках организационно-тактических мероприятий и т. п. Наибольшая вероятность установления личности преступника имеет место в том случае, когда уголовные дела по данной категории преступлений возбуждаются в результате реализации оперативных мероприятий. Указанные обстоятельства обусловливают необходимость взаимодействия оперативных работников и следователей на всех этапах расследования.

Важное значение имеет взаимодействие с экспертами (специалистами), обладающими знаниями в области информационных технологий, поскольку сотрудники правоохранительных органов не всегда владеют необходимыми знаниями и навыками в области информационных технологий, веб-разработки и сетевой безопасности. Привлечение специалиста в непроцессуальной форме возможно в рамках получения консультации. В ходе консультации следователь, исходя из сложившейся следственной ситуации, может выяснить возможные способы установления личности преступника, выявления идентификационных данных и обнаружения иных цифровых следов, необходимых для деанонимизации личности преступника. Однако наибольшую помощь в установлении личности преступника следователь получает в ходе процессуального взаимодействия. Например, при производстве допроса потерпевшего следователь может привлечь специалиста для помощи в постановке вопросов для наиболее полного выяснения обстоятельств и механизма совершения преступления, а также разъяснения IT-терминологии.

Также участие специалиста является обязательным при осмотре технического устройства потерпевшего. В рамках настоящего исследования мы не будем подробно рассматривать алгоритм действий специалиста, а остановимся лишь на тех аспектах участия специалиста, которые позволяют обнаружить ориентирующую информацию, необходимую для деанонимизации лица. Для обнаружения необходимой информации осмотру могут подлежать журнал входящих и исходящих звонков (в ходе осмотра которого можно обнаружить номер телефона), электронный почтовый ящик (в нем можно обнаружить адрес электронной почты, с которого отправляли фишинговые ссылки или иную информацию), приложения социальных сетей (в которых можно найти ценную информацию о никнеймах и идентификаторах пользователя (ID), которые присваиваются при регистрации и остаются неизменными). Именно идентификатор (ID) в большинстве случаев служит основным ориентиром при установлении аккаунта, поскольку он однозначно идентифицирует пользователя в базах данных. Также анализу подлежат журналы событий (log-файлы)[15], в которых можно обнаружить сообщения об ошибках, предупреждения, стек вызовов (англ. *stack trace*)[16], время, когда произошел сбой. Указанные сведения позволяют установить характер произошедшего события, последовательность действий и причинно-следственные связи между ними.

Помимо участия специалиста в следственных действиях, возможно его

[15] Журнал событий – встроенный инструмент, в который программа или система записывает свои действия. Он является своего рода хранилищем цифровых следов.

[16] Хронологическая запись всех вызовов функций, которые привели к ошибке в программе. Данная запись представлена в виде отчета, в котором содержится информация о типе ошибки, месте, где произошла ошибка (файл, строка и метод, где программа остановилась) и последовательности вызовов, которая привела к ошибке.

привлечение к проведению тактических операций по деанонимизации лица, например, при перехвате трафика в рамках проведения оперативно-розыскных мероприятий. Специалист может оказать содействие в применении программных и аппаратных инструментов перехвата сетевого трафика (*Wireshark, tcpdump*) и в анализе сетевого трафика, результаты которого позволяют обнаружить идентифицирующие данные и связанные с ними сведения: временные метки, IP-адреса, доменные имена, MAC-адрес сетевого интерфейса, идентификаторы мобильных устройств (IMEI, IMSI), учетные данные пользователя, сведения о браузере и операционной системе пользователя, данные геолокации [19, с. 367].

Отметим, что использование специальных знаний при расследовании компьютерных преступлений возможно не только при назначении компьютерно-технических экспертиз, но и при осуществлении организационно-тактических мероприятий, что свидетельствует об универсальной роли экспертов (специалистов) при расследовании преступлений в сфере компьютерной информации.

## V. Заключение

Обобщая изложенное, следует отметить, что сегодня сложно разработать единые рекомендации, которые бы позволили эффективно бороться с рассматриваемым видом противодействия, поскольку новые способы и средства совершения и сокрытия преступлений появляются достаточно быстро. Однако это не означает, что проанализированные виды и формы взаимодействия не позволят достичь положительных результатов сотрудникам правоохранительных органов, поскольку проведенное исследование может способствовать устранению рассмотренных в первой части статьи проблемных аспектов, обусловленных субъективными факторами, которые играют немаловажную роль в криминалистическом мышлении следователя и успешном раскрытии и расследовании преступлений.

Отметим и тот факт, что представленные способы получения идентификационных данных о личности преступника в рамках взаимодействия различных субъектов свидетельствуют о том, что успех преодоления информационной неопределенности на первоначальных этапах расследования будет заключаться только в комплексном взаимодействии путем объединения сил и средств, что позволит добиться эффективности в достижении целей по установлению личности преступников.

## Список литературы

1. Карпов Д. С., Ибрагимова З. А. Способы и средства обеспечения анонимности в глобальной сети Интернет // Правовая информатика. 2021. № 3. С. 60–67. DOI: https://doi.org/10.21681/1994-1404-2021-3-60-67

2. Jyothi K. K., Reddy B. I. Study on Virtual Private Network (VPN), VPN's Protocols and Security // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2018. Vol. 3, iss. 5. P. 919–932.

3. Kouachi A. I., Bachir A., Lasla N. Anonymizing Communication Flow Identifiers in the Internet of Things // Computers & Electrical Engineering. 2021. Vol. 91. DOI: https://doi.org/10.1016/j.compeleceng.2021.107063

4. Басыня Е. А., Хиценко В. Е., Рудковский А. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22, № 2. С. 45–51. DOI: https://doi.org/10.21293/1818-0442-2019-22-2-45-51

5. Тимофеев С. В. К вопросу добывания оперативно значимой информации в сети Интернет: проблемы и пути их решения // Криминалистика: вчера, сегодня, завтра. 2021. № 2 (18). С. 111–117. DOI: https://doi.org/10.24412/2587-9820-2021-2-111-117

6. Гайдин А. И., Головчанский А. В. Тактические средства преодоления способов анонимизации при расследовании сетевых преступлений // Вестник Воронежского института МВД России. 2024. № 2. С. 172–179.

7. Гаврилин Ю. В., Бедеров И. С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4 (60). С. 101–108. DOI: https://doi.org/10.24412/2072-9391-2021-460-101-108

8. Земцова С. И. Программные продукты, используемые для деанонимизации фактов совершения наркопреступлений с использованием цифровой валюты // Криминалистика – наука без границ: традиции и новации : материалы всерос. науч.-практ. конф., Санкт-Петербург, 26 нояб. 2020 г. / сост.: А. В. Бачиева, Э. В. Лантух. СПб. : С.-Петерб. ун-т М-ва внутр. дел Рос. Федерации, 2021. С. 112–115.

9. Данилкин И. А. Взаимодействие следственных и экспертно-криминалистических подразделений органов внутренних дел : моногр. М. : Юрлитинформ, 2010. 181 с.

10. Гайдин А. И. Проблемы взаимодействия органов предварительного расследования и представителей коммерческих организаций при производстве по уголовным делам о преступлениях в сфере информационно-телекоммуникационных технологий // Вестник Воронежского института МВД России. 2020. № 4. С. 151–156.

11. Антонов И. А., Узгорская И. А. Влияние информации, предоставленной операторами сотовой связи, на раскрытие и расследование различных категорий преступлений // Общество и право. 2015. № 2 (52). С. 185–189.

12. Сидорова К. С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. 2018. № 3 (74). С. 84–87. DOI: https://doi.org/10.24411/1999-6241-2018-12015

13. Sorbán K. The role of internet intermediaries in combatting cybercrime: Organisation and liabilities // Central and Eastern European E|Dem and E|Gov Days 2019 : proceedings of the Central and Eastern European E|Dem and E|Gov Days, May 2–3, 2019, Budapest / Editors: A. Nemeslaki, A. Prosser, D. Scola, T. Szádeczky. Budapest, 2019. P. 19–28. DOI: https://doi.org/10.24989/ocg.v335.1

14. Афонькин Г. П., Смирнов Е. В., Чемерчев Д. В. Основы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Полицейский вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2021. № 1 (4). С. 10–17.

15. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий // Труды академии управления МВД России. 2018. № 4 (48). С. 145–150.

16. Гайдин А. И. Особенности взаимодействия следователя с должностными лицами правоохранительных органов при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Вестник Воронежского института МВД России. 2020. № 3. С. 177–183.

17. Босхолов С. С., Брагина И. С., Сериков С. Н. Актуальные вопросы о необходимости создания условий для эффективной работы по раскрытию и расследованию преступлений, совершенных с использованием информационно–телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2021. № 3 (19). С. 69–76. DOI: https://doi.org/10.24412/2587-9820-2021-3-69-76

18. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. 2023. № 1 (37). С. 62–66.

19. Авдошин, С. М., Лазаренко А. В. Методы деанонимизации пользователей TOR // Информационные технологии. 2016. Т. 22, № 5. С. 362–372.

## *References*

1. Karpov D. S., Ibragimova Z. A. Ways and Means To Ensure Anonymity in the Global Internet Network. *Legal Informatics*. 2021;3:60-67. DOI: https://doi.org/10.21681/1994-1404-2021-3-60-67 (In Russ.)

2. Jyothi K. K., Reddy B. I. Study on Virtual Private Network (VPN), VPN's Protocols and Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2018;3(5):919-932.

3. Kouachi A. I., Bachir A., Lasla N. Anonymizing Communication Flow Identifiers in the Internet of Things. *Computers & Electrical Engineering*. 2021;91. DOI: https://doi.org/10.1016/j.compeleceng.2021.107063

4. Basinya E. A., Khitsenko V. E., Rudkovskiy A. A. Method To Identify Cybercriminals Using Network Analysis of Information Systems with Anonymization. *Proceedings of the TUSUR University.* 2019;22(2):45-51. DOI: https://doi.org/10.21293/1818-0442-2019-22-2-45-51 (In Russ.)

5. Timofeev S. V. To The Question of Gathering of Operately Significant Information on the Internet: Problems and Ways of Their Solution. *Forensics: Yesterday, Today, Tomorrow.* 2021;2:111-117. DOI: https://doi.org/10.24412/2587-9820-2021-2-111-117 (In Russ.)

6. Gaidin A. I., Golovchanskiy A. V. Tactical Means of Overcoming the Methods of Anonymization in the Investigation Network Crimes. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia.* 2024;2:172-179. (In Russ.)

7. Gavrilin Yu. V., Bederov I. S. Identification of Digital Currency Owners: Methodological Foundations. *Proceedings of the Management Academy of the Ministry of Interior of Russia*. 2021;4:101-108. DOI: https://doi.org/10.24412/2072-9391-2021-460-101-108 (In Russ.)

8. Zemtsova S. I. Software Products Used to Deanonymize the Circumstances of Drug Crimes Committed Using Digital Currency. In: Bachieva A. V., Lantukh E. V. (Comp.). *Criminalistics: A Science without Borders: Traditions and Innovations*. St. Petersburg: Saint Petersburg University of the Ministry of the Interior of Russia Publ.; 2021. P. 112–115. (In Russ.)

9. Danilkin I. A. *Cooperation between Investigative and Forensic Units of Internal Affairs Bodies*. Moscow: Yurlitinform Publ.; 2010. 181 p. (In Russ.)

10. Gaidin A. I. Problems of Interaction Between Preliminary Investigation Bodies and Representatives of Commercial Organizations in Criminal Proceedings on Crimes in the Field of Information and Telecommunications Technologies. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia.* 2020;4:151-156. (In Russ.)

11. Antonov I. A., Uzgorskaya I. A. Influence of the Information Provided By Cellular Operators on the Disclosure and Investigation of Various Categories of Offenses. *Society and Law*. 2015;2:185-189. (In Russ.)

12. Sidorova K. S. IP Address as One of Personal Identities in Criminal Investigation. *Psychopedagogics in Law Enforcement*. 2018;3:84-87. DOI: https://doi.org/10.24411/1999-6241-2018-12015 (In Russ.)

13. Sorbán K. The role of internet intermediaries in combatting cybercrime: Organisation and liabilities. In: Nemeslaki A., Prosser A., Scola D., Szádeczky T. (Eds.). *Central and Eastern European E|Dem and E|Gov Days 2019*. Budapest, 2019. P. 19–28. DOI: https://doi.org/10.24989/ocg.v335.1

14. Afonkin G. P., Smirnov E. V., Chemerchev D. V. The Basics of Countering Crimes Committees Using Information and Telecommunication Technologies. *Police Bulletin of the All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of the Russian Federation*. 2021;1:10-17. (In Russ.)

15. Gavrilin Yu. V. The Practice of Interaction's Organization in the Crimes' Investigation Committed with Using the Informational and Communication Technologies. *Proceedings of the Management Academy of the Ministry of Interior of Russia*. 2018;4:145-150. (In Russ.)

16. Gaidin A. I. Features of Interaction Between the Investigator and Law Enforcement Officials in the Investigation of Crimes in the Field of Information and Telecommunications Technologies. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia*. 2020;3:177-183. (In Russ.)

17. Boskholov S. S., Brugina I. S., Sericov S. N. Topical Issues on the Need To Create Conditions for Effective Work on the Detection and Investigation of Crimes Committed With the Use of Using Information and Telecommunications Technologies. *Forensics: Yesterday, Today, Tomorrow.* 2021;3:69-76. DOI: https://doi.org/10.24412/2587-9820-2021-3-69-76 (In Russ.)

18. Ivanov V. Yu. Using OSINT in Detecting and Investigating Crimes. *Bulletin of the Ural Law Institute of the Ministry of the Interior of Russia*. 2023;1:62-66. (In Russ.)

19. Avdoshin, S. M., Lazarenko A. V. TOR Users Deanonymization Methods. *Information Technologies*. 2016;22(5):362-372. (In Russ.)

## Информация об авторе

**Дарья Владимировна Воробьева,** адъюнкт адъюнктуры Уральского юридического института МВД России (ул. Корепина, 66, Екатеринбург, 620057, Российская Федерация); ORCID: https://orcid.org/0009-0007-5627-2450; e-mail: dacha_vorobyeva_13@mail.ru

## About the Author

**Daria V. Vorobyeva,** postgraduate student of the postgraduate courses at the Ural Law Institute of the Ministry of the Interior of Russia (66 Korepina str., Yekaterinburg, 620057, Russian Federation); ORCID: https://orcid.org/0009-0007-5627-2450; e-mail: dacha_vorobyeva_13@mail.ru

Поступила | Received 02.02.2026

Поступила после рецензирования и доработки | Revised 09.03.2026

Принята к публикации | Accepted 11.03.2026