Научная статья С. 147–154
УДК 343.9
DOI: 10.47475/2311-696X-2023-39-4-147-154

ОСОБЕННОСТИ РОЗЫСКНЫХ МЕРОПРИЯТИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Александр Сергеевич Киселев[1], **Горбунова Ксения Анатольевна**[2]
[1]*Государственный университет управления, Финансовый университет при Правительстве Российской Федерации, Москва, Россия*
alskiselev@fa.ru
https://orcid.org/0000-0002-5044-4721
[2]*Московский государственный юридический университет имени О. Е. Кутафина, Москва, Россия*
gorbynya.rambler.ru@yandex.ru

Аннотация. Вопросы совершенствования тактики розыскных мероприятий при расследовании преступлений в сфере компьютерной информации трудно переоценить. За последние годы ввиду значительного роста цифровизации неуклонно растет как количественные показатели преступлений в сфере компьютерной информации, так и их качественный уровень. Органам следствия становится сложнее собирать необходимые доказательства, обнаруживать электронно-цифровые следы, определять их авторство и устанавливать причинно-следственные связи. Современные оперативно-розыскные мероприятия предполагают наличие у сотрудников правоохранительных органов умений обнаружения и анализ цифровых данных, извлечения электронных следов, а также фиксацию этих данных в качестве улик.

Расследование преступлений в сфере компьютерной информации требует специализированных знаний и навыков, чтобы эффективно противостоять новым методам и технологиям, используемым правонарушителями. Актуальность тактики розыска обусловлена необходимостью адаптироваться к постоянно меняющейся киберугрозе и обеспечивать безопасность информационных систем.

Определено, что правоохранительным органам необходимо постоянно совершенствовать свои навыки и обогащать знания, очевидна необходимость соответствующего материально-технического оснащения, предполагающего наличие специализированных инструментов. Особенно важна модернизация тактики розыска подозреваемых.

Выявлено, что прослушивание телефонных переговоров является важным элементом в проведении оперативно-розыскных мероприятиях. Прослушивание предполагает установку аудиоследящих устройств на телефонные линии связи, а также заключение соглашения с операторами связи для получения доступа к интернет-трафику и телефонным разговорам. Однако существуют значительные риски злоупотребления полномочиями со стороны правоохранительных органов. К сожалению, в законе не определен перечень критериев, по которым можно установить, следует ли применять прослушивание в конкретном случае или нет. Это создает угрозы персональных данных пользователей и вносит неопределённость в правоприменительную деятельность.

Ключевые слова: тактика следственных органов, расследование киберпреступлений, преступления в сфере компьютерной информации, розыск, тактика розыска киберпреступников, следственные мероприятия, оперативно-розыскные мероприятия

Для цитирования: Киселев А. С., Горбунова К. А. Особенности розыскных мероприятий при расследовании преступлений, совершаемых в сфере компьютерной информации // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 147–154. DOI: 10.47475/2311-696X-2023-39-4-147-154

Research article

PECULIARITIES OF SEARCH MEASURES IN THE INVESTIGATION OF CRIMES COMMITTED IN THE SPHERE OF COMPUTER INFORMATION

Aleksandr S. Kiselev[1], **Kseniya A. Gorbunova**[2]
[1]*State University of Management, Financial University under the Government of the Russian Federation, Moscow, Russia*
alskiselev@fa.ru
https://orcid.org/0000-0002-5044-4721
[2]*Moscow State Law University named after O. E. Kutafin, Moscow, Russia*
gorbynya.rambler.ru@yandex.ru

Abstract. It is difficult to overestimate the issues of improving the tactics of investigative measures in the investigation of crimes in the field of computer information. In recent years, due to the significant growth of digitalization, both quantitative indicators of crimes in the field of computer information and their qualitative level have been steadily increasing. It becomes more difficult for investigative bodies to collect the necessary evidence, detect electronic and digital traces, determine their authorship and establish cause-and-effect relationships. Modern operational investigative measures assume that law enforcement officers have the skills to detect and analyze digital data, extract electronic traces, as well as record these data as evidence.

The investigation of crimes in the field of computer information requires specialized knowledge and skills to effectively counter the new methods and technologies used by offenders. The relevance of the search tactics is due to the need to adapt to the ever-changing cyber threat and ensure the security of information systems.

It is determined that law enforcement agencies need to constantly improve their skills and enrich their knowledge, the need for appropriate material and technical equipment, assuming the availability of specialized tools, is obvious. It is especially important to modernize the tactics of searching for suspects.

It has been revealed that wiretapping is an important element in conducting operational search activities. Listening involves installing audio tracking devices on telephone communication lines, as well as concluding an agreement with telecom operators to gain access to Internet traffic and telephone conversations. However, there are significant risks of abuse of authority by law enforcement agencies. Unfortunately, the law does not define a list of criteria by which it is possible to determine whether listening should be used in a particular case or not. This creates threats to users' personal data and introduces uncertainty into law enforcement activities.

Keywords: tactics of investigative bodies, investigation of cybercrimes, crimes in the field of computer information, search, tactics of searching for cybercriminals, investigative measures, operational search measures

For citation: Kiselev AS, Gorbunova KA. Peculiarities of search measures in the investigation of crimes committed in the sphere of computer information. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2023;(4):147-1540. DOI: 10.47475/2311-696X-2023-39-4-147-154 (In Russ.)

Введение

Противоправные действия в сфере компьютерной информации — это преступления, связанные с использованием электронного оборудования и программного обеспечения, включая хакерство, интернет-мошенничество и др. Расследование таких преступлений требует применения специальных методов и тактики.

Для поиска причин и условий совершения преступлений в компьютерной среде можно выделить следующие категории лиц: киберпреступники, обладающие высокой квалификацией и разрабатывающие, применяющие вредоносные программы; обычные люди, которые преднамеренно публикуют в интернете ложные объявления о продаже ценных вещей по низкой цене, вводят покупателей

в заблуждение, используют скаченное вредоносное программное обеспечение для похищения чужих данных и др. Из этого можно сделать вывод, что для совершения преступлений в сфере компьютерной информации не всегда необходимо наличие специальных знаний, вполне достаточно использования компьютерной техники и выхода в интернет.

Невысокий уровень эффективности раскрытия преступлений в сфере компьютерной информации связан с несовершенством нормативных регламентов, сложностью фиксации электронно-цифровых следов, отставанием следственной практики от передовых технологий злоумышленников. Отсутствие материальных следов в процессе совершения преступления, а также наличие различных способов его реализации являются одними из причин латентности компьютерных преступлений. Вредоносное программное обеспечение может быть создано в одной стране, а использовано по всему миру, что затрудняет определение территориальных границ.

Основной текст статьи

При проведении расследования необходимо провести анализ следов не только на технических устройствах (компьютерах, ноутбуках, планшетах, смартфонах), но и в каналах связи, которые они используют, таких как протоколы соединений, отправленные сообщения и т. д. Файлы могут содержать изображения, видео, программное обеспечение и пр. Для получения вышеуказанных данных требуется проведение оперативно-розыскных мероприятий. Полученная оперативными сотрудниками информация передается для использования органами дознания, следствия или в суд. Следовательно, уголовные дела, связанные с преступлениями в сфере компьютерной информации, возбуждаются на основе сведений, полученных в ходе проведения оперативно-розыскных мероприятий (далее — ОРМ) как предупредительных, так и в регулярном порядке, а также по факту уже совершенного преступления.

В п. 2 ч. 3 ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлен срок до 6 месяцев для хранения оператором связи текстовых сообщений пользователей, голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей сети интернет с момента окончания их приема, передачи, доставки и (или) обработки. Это способствует эффективному проведению ОРМ и следственных действий правоохранительными органами[1]. Полученные результаты помогают выявить скрытые сведения о способах совершения преступления и участии других лиц, которые могут быть неизвестны подозреваемому, но являться участниками противоправной деятельности. Это, в свою очередь, позволяет предотвратить отклонение доказательств, полученных до судебного процесса.

Ю. И. Юрина отмечает: «После возбуждения уголовного дела составляется план производства следственно-оперативных мероприятий, его последовательность с учетом полученной информации, собранной в материалах проверки, в том числе определяется тактика допроса свидетелей и подозреваемого лица, избрание меры пресечения» [12, с. 56].

Использование ОРМ «Получение компьютерной информации» для сбора электронных данных может рассматриваться как дополнительный способ подтверждения улик в уголовном процессе и позволяет обеспечить высокий уровень защиты со стороны правоохранительных органов в отношении средств сбора данных.

Схожими по своей сути и содержанию к «Получению компьютерной информации» являются ОРМ «Прослушивание телефонных переговоров» и «Снятие информации с технических каналов связи», которые ранее отражались в Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[2].

Снятие информации с технических каналов связи — это процесс получения данных о сообщениях, передаваемых через средства связи, с целью их анализа и использования в оперативно-розыскных мероприятиях, может включать перехват, запись и анализ электронных сообщений, телефонных звонков, сообщений через социальные сети и другие средства связи. Снятие информации с технических каналов связи может применяться в следственной деятельности для пресечения и раскрытия преступлений [11, с. 325]. Указанные оперативно-розыскные мероприятия осуществляется только на основании судебного решения, с привлечением оперативно-технических средств и сил органов внутренних дел и Федеральной службы безопасности.

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102108264&intelsearch=&firstDoc=1 (дата обращения: 18.04.2023).

[2] Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ // Российская газета. 1995. 18 авг. (№ 160).

Основные тактические приемы при расследовании преступлений в сфере компьютерной информации могут быть разделены на следующие этапы:

— *Сбор информации*. На этом этапе следователи собирают все доступные данные о преступлении и его возможных участниках, включая сбор данных о взламываемых системах, сетевых узлах, аккаунтах в социальных сетях, электронной почте и т. д.

— *Анализ информации*. После сбора информации следователи анализируют данные, полученные из разных источников, чтобы выявить возможные связи, паттерны и отношения между различными участниками преступления.

— *Идентификация подозреваемых*. На основе собранной информации и ее анализа следователи могут выявить подозреваемых и узнать больше о их мотивах и возможных действиях.

— *Использование слежения и контроля*. Для получения дополнительной информации следователи могут применять различные методы, например, мониторинг телефонных звонков, компьютерных действий, интернет-трафика и т. д.

— *Поиск доказательств*. После того как следователи идентифицировали подозреваемых и получили информацию о них, они приступают к формированию доказательственной базы, которая подтверждают вину подозреваемых. При этом, данные могут быть получены из различных источников, включая компьютеры, телефоны, электронную почту и т. д.

— *Арест и судебное разбирательство*. После того, как следователи собрали достаточно доказательств, они могут согласовать с судом арест подозреваемого.

Таким образом, тактика розыскных мероприятий при расследовании компьютерных преступлений включает сбор и анализ информации, идентификацию подозреваемых, использование слежения и контроля, поиск доказательств, арест и судебное разбирательство.

Розыскные мероприятия при расследовании компьютерных преступлений могут включать в себя следующие действия:

1. Изъятие компьютерной техники: ПК, ноутбуки, смартфоны, планшеты, внешние жесткие диски и другие устройства хранения информации.

2. Копирование данных с изъятых устройств для получения полной картины происходящего является важным розыскным мероприятием при расследовании компьютерных преступлений. Копирование данных (или дископия) позволяет сохранить информацию, находящуюся на компьютере подозреваемого, без ее изменения или повреждения.

В целом, копирование информации является важным розыскным мероприятием, которое помогает экспертам провести анализ и исследование данных в деталях, что, в свою очередь, способствует улучшению качества расследования компьютерных преступлений. При этом, как подчеркивают Е. Р. Россинская и И. А. Рядовский, «формальный подход к следственному действию может повлечь безвозвратную утрату доказательственной информации, что обусловлено в первую очередь такими свойствами цифровых следов, как высокая скорость модификации в вычислительных системах, а также возможность их уничтожения либо фальсификации с целью сокрытия преступления» [9, с. 106].

1. Обыск помещений — особое мероприятие, которое может быть проведено для поиска компьютерной техники и других устройств хранения данных. В ходе проведения мероприятия следователи проводят досмотр и изъятие различных объектов и устройств, связанных с компьютерным преступлением, например: компьютеров, ноутбуков, внешних накопителей данных, USB-флешек, мобильных телефонов, смарт-карт и т. д.

При обыске следователи также имеют право получать информацию от владельцев помещения о паролях и доступах к электронным устройствам, а также могут запрашивать доступ к защищенной информации на компьютерах. Однако при этом необходимо соблюдать законность проведения обыска и защиту прав и свобод граждан. Такое мероприятие проводиться только при наличии судебного разрешения. Следователи также должны соблюдать приватность персональной информации, содержащейся на обыскиваемых устройствах, опечатывать материальные носители информации и хранить в сейфе.

2. Анализ изъятых данных, направленный на исследование найденной информации для выявления фактов преступления.

Задачи указанного мероприятия при расследовании компьютерных преступлений заключаются в следующем:

— определение формы преступления и его масштаба;

— установление личности подозреваемого;

— предоставление доказательств в суде.

Вне всякого сомнения, «в результате анализа данных выполняются действия, направленные на извлечение информации

об исследуемом объекте, а также получение новых знаний о событии преступления» [4, с. 178].

3. Экспертиза данных помогает оценить достоверность найденной информации. Это мероприятие играет важную роль в расследовании компьютерных преступлений — позволяет собрать, анализировать и интерпретировать различные типы данных, хранящиеся на компьютерах или других устройствах в рамках предъявления обвинений в компьютерном преступлении.

Обычно специалисты по экспертизе информации занимаются изучением данных, связанных с доступом к компьютерным системам, интернет-сайтам или электронной почте. Эти материалы могут включать в себя историю браузера, файлы, находящиеся на жестком диске, записи о входах в систему, данные, передаваемые по сети, и мн. др. Во время экспертизы данных специалисты применяют различные методы и технологии, например, снятие образов жестких дисков, использование программного обеспечения для анализа данных и ручной анализ информации.

4. Наблюдение и прослушивание используются при подозрении, что преступление совершится в будущем.

Такой способ в качестве розыскных мероприятий можно использовать, но только при соблюдении определенных условий и законодательных норм. В постановлении Пленума Верховного суда Российской Федерации от 1 июня 2017 года № 19 г. Москва «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (ст. 165 УПК РФ)»[1] разъясняется, когда следователи могут прослушивать.

Прослушивание является мерой, которая должна применяться в строго оговоренных случаях. При этом Пленум ВС РФ пока не дает конкретного перечня ситуаций, при которых прослушивание можно считать допустимым мероприятием при осуществлении следственных действий. Вполне возможно, что с целью обеспечения национальной безопасности, противодействия терроризму и предотвращения крупных тяжких преступлений, направленных против основ конституционного строя, допустимо использование прослушивания, поскольку другими способами получить доказательства может быть невозможно, а степень опасности последствий преступлений может носить беспрецедентный характер.

По поводу наблюдения в своей работе А. П. Жусипбекова отмечает следующее: «Наиболее широко используемым в досудебном производстве методом является наблюдение, с помощью которого производится большое количество следственных действий: обыск, выемка, осмотр места происшествия, осмотр вещей и предметов, допрос, очная ставка, предъявление для опознания и т. п.» [3, с. 62–63]. Сегодня принципиально меняются подходы к проведению некоторых следственных действий. Так, Ю. Н. Соколов в своей работе делает акцент на том, что «наблюдение как следственное действие все чаще производится в электронной форме» [10, с. 304].

Эти меры могут быть применены, например, при подозрении в совершении кибератак на объекты критической инфраструктуры или других компьютерных преступлений, посягающих на общественную безопасность. Однако для их применения следует получить специальное разрешение суда, которое будет основано на аргументации необходимости проведения наблюдения и прослушивания. Таким образом, наблюдение может быть удачной розыскной мерой при расследовании компьютерных преступлений, но в процессе их применения необходимо следовать требованиям законодательства, защищая каждого человека. Кроме того, стоит помнить о необходимости соблюдения прав каждого на частную жизнь. Ведь как справедливо замечают исследователи, «на практике данные оперативно-розыскные мероприятия могут нарушать и нередко нарушают конституционные права граждан» [7, с. 196].

Прослушивание телефонных переговоров является одним из самых важных оперативно-розыскных мероприятий и используется правоохранительными органами для получения информации о преступных действиях и нарушениях закона, а также для обеспечения национальной безопасности. Существует несколько способов проведения прослушивания телефонных разговоров, включая применение специального оборудования и программного обеспечения, установку аудиоследящих устройств на телефонные линии, а также заключение соглашения с операторами связи для получения доступа к интернет-трафику и телефонным разговорам.

[1] О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ) : постановление Пленума Верховного суда Российской Федерации от 01.06.2017 № 19 // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/71589794/ (дата обращения: 18.04.2023).

А. В. Ковальчук указывает: «На практике сначала судом даётся разрешение о проведении таких ОРМ в отношении неустановленных лиц. В ходе анализа полученных данных устанавливаются лица, возможно причастные к преступлению, совершённому в указанном месте и в установленное время. После чего органы, осуществляющие ОРД, обращаются за разрешением на проведение ОРМ в отношении конкретных лиц и по определённым номерам телефонов» [5, с. 53–54]. Некоторые исследователи убеждены, что требуется разработка общих характерных признаков, при наличии которых проведение подобных ОМР будет считаться обоснованным [6, с. 107].

Указанное ОРМ признается одним из самых эффективных способов раскрытия преступлений и имеет наиболее детализированную регламентацию в федеральном законе «Об оперативно-розыскной деятельности». Сегодня преступники все реже используют традиционные каналы телефонной связи, поскольку у них вызывает опасение быть прослушанными со стороны правоохранительных органов. Современные преступники пользуются различными методами шифрования, голосовыми чатами на игровых платформах, где риск прослушивания сводится к минимуму. Даже при наличии разрешения суда на проведение таких ОРМ получить информацию о переговорах бывает очень сложно. Более того, на практике в определенных ситуациях при использовании подозреваемыми комбинированных видов связи возникают трудности в определении разницы между проведением таких ОРМ, как «Прослушивание телефонных разговоров» и «Снятие информации с технических каналов связи» [8, с. 483–485]. В некоторых случаях определить содержание мероприятия «Получение компьютерной информации» и связать его с уже упомянутыми мероприятиями может быть еще более сложной задачей.

Развитие коммуникационных услуг существенно прогрессирует благодаря распространению портативных устройств с доступом в интернет. При использовании сетевых коммуникаций соединение устанавливается через комплексную инфраструктуру, где одновременно доступны различные коммуникационные сервисы, предоставляемые разными операторами, что отличается от обычной телефонии. Некоторые из них могут находиться за пределами страны и не обязаны предоставлять информацию в ответ на запросы от отечественных правоохранительных органов.

Применение специализированных мобильных устройств с возможностью зашифрованной связи вызывает особые трудности в борьбе с преступниками. Приведем в качестве примера широкого предоставления мобильной шифровки для организованной преступности доказательства из дела Федерального Бюро Расследований США (ФБР) в отношении деятельности канадской компании Phantom Secure, которая обслуживала более 20 тыс. клиентов.

Расследование ФБР США в отношении работы этой компании связано с ее предполагаемым участием в организации преступной деятельности, включая наркоторговлю и оружейный бизнес. Phantom Secure является производителем защищенных мобильных устройств, которые, по предположению правоохранительных органов, используются криминальными группировками для шифрования своей коммуникации и координации преступных действий[1].

Специалисты компании Phantom Secure предоставляли зашифрованные телефоны Blackberry, специально предназначенные для использования криминальными группировками и наркоторговцами. Они удаляли функции GPS, камеры и микрофона и устанавливали программное обеспечение PGP и Advanced Encryption Standard (AES) для шифрования сообщений и звонков, что делала прослушивание последних невозможным.

Это обеспечивало высокий уровень «безопасности» преступных действий от правоохранительных органов. Один из крупнейших провайдеров зашифрованной цифровой связи EncroChat обслуживал множество пользователей, причастных к преступной деятельности, а также предлагал продажу телефонов с обеспечением анонимности связи. Однако в июне 2020 года серверы EncroChat были взломаны, благодаря чему правоохранительные органы многих стран смогли получить доступ к зашифрованным сообщениям. В результате было раскрыто множество преступных схем, включая наркоторговлю, отмывание денег, оружейную торговлю и организованную преступность. Крупнейшие аресты были проведены в Великобритании, Нидерландах, Франции и Италии, при этом полиция обнаружила большое количество наркотиков, оружия и денег. В результате EncroChat был закрыт, а многие представители организованной преступности были арестованы.

Специалисты утверждают, что это свидетельствует о необходимости непрерывного

[1] Cox J. The FBI Tried to Plant a Backdoor in an Encrypted Phone Network // VICE. URL: https://www.vice.com/en/article/pa73dz/fbi-tried-to-plant-backdoor-in-encrypted-phone-phantom-secure (дата обращения: 16.08.2023).

увеличения возможностей правоохранительных органов для работы с зашифрованной информацией в ходе уголовных расследований в соответствии с действующим законодательством, что особенно важно при осуществлении оперативно-розыскной деятельности в киберпространстве. Проблема, связанная с использованием криминальными элементами современных технологий шифрования, становится особенно актуальной. Это обстоятельство отмечается рядом отечественных ученых [2, с. 348–357; 1, с. 387–388].

В последнее время в зарубежной специальной литературе соответствующая проблема получила название «Going Dark» — это термин, который используется для описания ситуации, когда правоохранительные органы не могут законным путем получить доступ к зашифрованным данным на устройствах или в приложениях. Такое положение может быть обусловлено использованием технологий шифрования, анонимных мессенджеров, сервисов облачного хранения и других технологий приватности и безопасности. Следователь может обратиться к провайдерам интернет-услуг, чтобы установить тех, кто использовал определенный IP-адрес для совершения преступления, однако этого может быть недостаточно.

В целом ОРМ «Получение компьютерной информации» дает возможность более эффективно способствовать выявлению, расследованию и раскрытию преступлений, связанных с компьютерными и телекоммуникационными технологиями.

Это мероприятие, наряду со «Снятием информации с технических каналов связи» и «Прослушиванием телефонных переговоров», относится к классу оперативно-технических мероприятий. Как известно, для их технического обеспечения на сетях документальной электросвязи, используемых с целью предоставления услуг передачи данных телематических служб, создана Система технических средств по обеспечению оперативно-розыскных мероприятий. Ее технические требования регламентированы приказом Государственного комитета РФ по связи и информации от 27 марта 1999 года № 47[1].

Действия оперативников при этом направлены на проникновение в аппаратные компоненты компьютерных систем (ПК, периферийные устройства, ИТКС, носители информации), принадлежащие лицам, которых подозревают в совершении преступлений. Они используют специальные технические или программные методы для копирования компьютерной информации, которая является оперативно важной.

Вместе с тем, существуют частные случаи, когда искомая информация на компьютере может быть получена и без судебного решения или без принятия мотивированного решения со стороны компетентного руководителя правоохранительных органов. Например, в ситуации, если подозреваемый был пойман на месте преступления в общественном или другом месте и оперативник выполняет обыск в его личном техническом средстве (компьютер, смартфон, планшет или другое аналогичное устройство).

Заключение

Таким образом, не остается сомнений в том, насколько важным стало умение сотрудников правоохранительных органов получить доступ к скрытым преступниками компьютерным данным, выявить главные закономерности и возможные места их сосредоточения, а также извлечь всю ценную информацию из массива компьютерных данных, при необходимости в некоторых ситуациях оставаясь анонимным. Установлено, что основные тактические мероприятия при расследовании преступлений в сфере компьютерной информации могут быть разделены на следующие этапы: сбор информации, анализ данных, идентификация подозреваемых, использование слежения и контроля, поиск доказательств, проведение ареста и судебного разбирательства. Определено, что розыскные мероприятия при расследовании компьютерных преступлений могут включать в себя следующие действия: изъятие компьютерной техники, копирование данных, обыск помещений, анализ изъятых данных, экспертизу данных, наблюдение и прослушивание, арест или задержание подозреваемого, сбор дополнительных свидетельств, привлечение свидетелей и допросы, а также межведомственное сотрудничество. При этом особое внимание стоит уделять квалификации и навыкам сотрудников правоохранительных органов.

[1] Об утверждении Общих технических требований к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на сетях (службах) документальной электросвязи : приказ Госкомсвязи РФ от 27.03.1999 № 47 // Бюллетень Министерства Юстиции Российской Федерации. 1999. № 7.

Список источников

1. Бабенко С. В., Садовая Д. С. Проблемы теории и практики прокурорского надзора за производством предварительного расследования киберпреступлений // Евразийский юридический журнал. 2021. № 2 (153). С. 387–388.

2. Гусейнов Т. А. Проблемы и особенности расследования киберпреступлений // Вопросы российской юстиции. 2020. № 6. С. 348–357.

3. Жусипбекова А. М. Наблюдение как метод исследования доказательств в досудебном производстве по уголовному делу // Молодой учёный : сб. статей IX Международного научно-исследовательского конкурса. Пенза : Наука и Просвещение (ИП Гуляев Г. Ю.), 2022. С. 62–64.

4. Карданов Р. Р., Курин А. А. Аналитическая обработка криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 173–181.

5. Ковальчук В. А. Отдельные вопросы проведения ОРМ, ограничивающих конституционные права граждан // Вопросы взаимодействия правоохранительных органов и их подразделений при раскрытии и расследовании преступлений : сб. тр. межведомственного круглого стола (Тверь, 06 апреля 2022 года) / под общ. ред. С. В. Клещёва, Ю. В. Сидорова, Д. О. Туманова, Е. А. Доценко. Тверь : Тверской гос. ун-т, 2022. С. 52–58.

6. Манукян Н. Р. Некоторые проблемы применения прослушивания, контроля и перехвата телефонных переговоров как оперативно-розыскного мероприятия в соотношении с конституционными правами человека // Научная школа уголовного процесса и криминалистики Санкт-Петербургского государственного университета : материалы XIII Международной конференции (Санкт-Петербург, 24–25 июня 2021 года) / под ред. Н. П. Кирилловой, В. Д. Пристанскова Н. Г. Стойко, В. Ю. Низамова. Часть 2. Москва : Русайнс, 2022. С. 107–115.

7. Могилкина С. Н., Шаров Р. А. Спорные вопросы осуществления оперативно-розыскной деятельности: закон и практика // Эпомен. 2020. № 48. С. 193–199.

8. Никулина А. А. Разграничение ОРМ «получение компьютерной информации» и «снятие информации с технических каналов связи» // Проблемы совершенствования российского законодательства : сб. тезисов Всероссийской (с международным участием) научной конференции курсантов, слушателей и студентов (Барнаул, 11 апреля 2019 года) / под редакцией Ю. В. Анохина. Барнаул : Барнаульский юрид. ин-т МВД РФ, 2019. С. 483–485.

9. Россинская Е. Р., Рядовский И. А. Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // LexRussica (Русский закон). 2021. Т. 74, № 9. С. 102–118.

10. Соколов Ю. Н. Электронное наблюдение как комплексное следственное действие // Евразийский юридический журнал. 2019. № 7 (134). С. 304–306.

11. Фролкин Н. П., Яковец Е. Н. Характерные особенности оперативно-розыскных мероприятий «снятие информации с технических каналов связи» и «получение компьютерной информации» // Эпомен. 2022. № 68. С. 325–355.

12. Юрина Ю. И. Особенности тактики производства первоначальных следственных действий и оперативно-розыскных мероприятий, проводимых при установлении лица, совершившего незаконный сбыт наркотических средств с использованием электронных и информационно-телекоммуникационных сетей (включая сеть «Интернет») // Актуальные проблемы современности. 2021. № 2 (32). С. 54–59.

ВКЛАД АВТОРОВ
Вклад авторов равноценный.

CONTRIBUTION OF AUTHORS
Contributions by the authors are equal.

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует.

CONFLICT OF INTEREST
There is no conflict of interest.

Дата поступления статьи / Received: 21.09.2023.
Дата рецензирования статьи / Revised: 15.11.2023.
Дата принятия статьи к публикации / Accepted: 05.12.2023.