Краснодарский университет МВД России

АЛГОРИТМ РЕАЛИЗАЦИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» ПРИ ВЫЯВЛЕНИИ, ПРЕДУПРЕЖДЕНИИ, ПРЕСЕЧЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА

Методические рекомендации

Краснодар
2019

УДК 343.985
ББК 67
А45

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *А. Л. Осипенко, А. Г. Белый, В. В. Стукалов, Е. В. Запорожец, Н. П. Голяндин, Д. В. Гуров, А. И. Мещерин*.

Рецензенты:
А. В. Ковалев, кандидат юридических наук, доцент (Рязанский филиал Московского университета МВД России им. В.Я. Кикотя);
И. Л. Алексеенко (ЦЭП ГУ МВД России по Краснодарскому краю).

А45 **Алгоритм реализации оперативно-розыскного мероприятия «получение компьютерной информации» при выявлении, предупреждении, пресечении и раскрытии преступлений экстремистской направленности и террористического характера** : методические рекомендации / сост. : А. Л. Осипенко, А. Г. Белый, В. В. Стукалов и др. – Краснодар : Краснодарский университет МВД России, 2019. – 24 с.

ISBN 978-5-9266-1525-5

В методических рекомендациях рассматриваются сущность, организация и тактика проведения сотрудниками подразделений по противодействию экстремизму и терроризму оперативно-розыскного мероприятия «получение компьютерной информации».

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.985
ББК 67

ISBN 978-5-9266-1525-5

ВВЕДЕНИЕ

В настоящее время в России ведется активная борьба с экстремизмом и терроризмом, в том числе в сети Интернет. Российское законодательство содержит конкретные правовые нормы, предоставляющие правоохранительным органам значительные возможности для противодействия преступлениям экстремистской направленности и террористического характера. Эти нормы содержатся в ряде законов и ведомственных нормативных актов. Необходимо отметить, что законодательство в данной сфере постоянно совершенствуется. Так, 1 февраля 2014 года вступил в силу Федеральный закон от 28 февраля 2013 г. № 398-ФЗ «О внесении изменений в Федеральный закон ”Об информации, информационных технологиях и о защите информации”»[1], который предусматривает немедленное и внесудебное принятие мер по ограничению доступа к информационным ресурсам, распространяющим экстремистские материалы. С момента вступления его в силу все сайты, содержащие призывы к массовым беспорядкам, к осуществлению экстремистской деятельности, блокируются в течение часа после получения предписания прокурора.

В ноябре 2014 года Президентом России утверждена Стратегия противодействия экстремизму в Российской Федерации до 2025 года[2], в которой определены основные направления государственной политики по противодействию экстремизму и мероприятия по ее реализации.

Федеральный закон от 28 июня 2014 года № 179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» ввел уголовное наказание за финансирование экстремистской деятельности (ст. 282.3 УК РФ), а также призывы к экстремизму в Интернете (ч. 2 ст. 280 УК РФ).

Несмотря на продолжающиеся масштабные изменения в действующем законодательстве, недостаточно внимания уделяется вопросам процедурно-правовой регламентации доступа к компьютерным данным в интересах оперативно-розыскной деятельности.

---

[1] См.: О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: федер. закон от 28 декабря 2013 г. № 398-ФЗ. URL: http://consultant.ru

[2] См.: Стратегия противодействия экстремизму в Российской Федерации до 2025 года: указ Президента РФ от 28 ноября 2014 г. № Пр-2753. URL: http://consultant.ru

Федеральный закон от 6 июля 2016 года № 374-ФЗ «О внесении изменений в Федеральный закон ”О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[1] внес изменения в ст. 6 Федерального закона от 12 августа 1996 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД), добавив новое оперативно-розыскное мероприятие (далее – ОРМ) – получение компьютерной информации. Однако ни в указанных федеральных законах, ни в ведомственных приказах содержание и порядок проведения нового ОРМ не определены.

Таким образом, возникла парадоксальная ситуация, когда наименование мероприятия закреплено в профильном законе, регулирующем общественные отношения, возникающие в процессе осуществления оперативно-розыскной деятельности, т. е. юридически возможность проведения получения компьютерной информации существует, а содержательная часть и процессуальный порядок реализации данного ОРМ фактически не регламентированы.

Отсутствие пошагового алгоритма реализации данного ОРМ и непонимание всего спектра оперативных возможностей в сфере противодействия преступности у оперативных сотрудников приводят к определенным трудностям при его осуществлении.

Так, например, анализ практики деятельности оперативных подразделений ГУ МВД России по Краснодарскому и Ставропольскому краям показал, что с момента внесения соответствующих изменений в Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (далее – «О противодействии терроризму»), Закон об ОРД и отдельные законодательные акты Российской Федерации, устанавливающие дополнительные меры противодействия терроризму и обеспечения общественной безопасности, такое ОРМ, как «получение компьютерной информации», не инициировалось и не проводилось. Фактически же при противодействии экстремизму и терроризму реализовывались иные ОРМ, тем или иным образом связанные с получением компьютерной информации (например, наведение справок, снятие информации с технических каналов связи, обследование помещений, зданий, сооружений,

[1] URL: http://consultant.ru

участков местности и транспортных средств (электронный досмотр) и др.).

Исходя из вышеизложенного коллектив авторов Краснодарского университета МВД России и его филиалов разработал методические рекомендации, которые облегчат понимание сотрудниками, осуществляющими оперативно-розыскную деятельность, важности данного ОРМ, позволят повысить эффективность и результативность его проведения при выявлении, предупреждении, пресечении и раскрытии преступлений экстремистской направленности и террористического характера, а также исключить возможные нарушения и ошибки при составлении необходимых оперативно-служебных документов.

1. ПОНЯТИЕ, СОДЕРЖАНИЕ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Использование ОРМ «получение компьютерной информации» позволяет расширить границы осуществления оперативно-розыскной деятельности, связанной с противодействием экстремизму и терроризму, т.к. сотрудники оперативных подразделений получают возможность не только обнаруживать и документировать оперативно значимую информацию о преступлениях экстремистской направленности и террористического характера, но и с помощью сети Интернет определять объекты (конкретные ресурсы), на которых она размещается.

Объектами ОРМ «получение компьютерной информации» в рассматриваемой сфере деятельности являются:

– лица, подготавливающие, совершающие или совершившие конкретные преступления экстремистской направленности и террористического характера;

– лица, располагающие (владеющие) оперативно значимой информацией о подготавливаемых, совершаемых или совершенных преступлениях экстремистской направленности и террористического характера, а также о лицах, их подготавливающих, совершающих или совершивших;

– криминогенные объекты и места, где достаточно велика вероятность совершения преступлений экстремистской направленности и террористического характера;

– события и факты, вызывающие оперативный интерес или содержащие признаки преступлений данного вида.

В процессе выявления оперативно значимой информации о преступлениях экстремистской направленности и террористического характера проведение ОРМ «получение компьютерной информации» поможет оперативному сотруднику собрать необходимую

информацию о том, на какие интернет-сайты заходил разрабатываемый и под каким никнеймом[1], с какими лицами вел интернет-переписку, какими интернет-источниками пользовался, какую информацию искал и получил, а также определить состав и характер группы, в которую входит разрабатываемый, ее внутренние и внешние связи, выявить используемые адреса электронной почты, номера сотовых и иных телефонов, установить идентификационные данные интернет-подключения и др. При использовании сети Интернет для совершения преступлений экстремистской направленности и террористического характера, как правило, видимые следы преступления обнаружить нельзя, в отличие от виртуальных следов, которые остаются в персональном компьютере, мобильном устройстве, электронных почтовых ящиках, а также таких мессенджерах, получивших широкое распространение у интернет-пользователей, как Viber, WhatsApp, Telegram и т.д. Поэтому, несмотря на сложности, возникающие при проведении поисковых мероприятий и сборе необходимых доказательств, в процессе обнаружения компьютерной информации и фиксации ее на материальных носителях важно обеспечить возможность ее дальнейшего использования в оперативно-розыскной деятельности и уголовном судопроизводстве.

Прежде чем решить данную задачу, необходимо установить, что законодатель понимает под ОРМ «получение компьютерной информации», а затем представить механизм его реализации.

Получение компьютерной информации – это ОРМ, заключающееся в использовании технических средств и информационных технологий для исследования компьютерных систем с целью обнаружения и документирования виртуальных и материальных следов, свидетельствующих о подготовке или совершении преступлений, которые могут содержаться в компьютерных системах в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

ОРМ «получение компьютерной информации» отражает не способ ее получения, а форму, в которой она представлена. Именно этим данное ОРМ отличается от схожих с ним ОРМ, часть из которых допускает получение результатов ОРМ в виде компьютерных

[1] Никнейм (от англ. nickname – сетевое имя) – псевдоним, который используется при виртуальном общении в Интернете (например, на форумах, в чатах, на блогах).

файлов (наведение справок, снятие информации с технических каналов связи, сбор образцов для сравнительного исследования и др.). Определение понятия «компьютерная информация»[1], закрепленное в ст. 272 УК РФ, через форму ее представления, а не путем перечисления средств ее хранения, обработки и передачи, ограничивает возможности его применения, поскольку спектр таких средств постоянно изменяется и расширяется. Независимость электрических сигналов от средств хранения, обработки и передачи отмечается в примечании к ст. 272 УК РФ, что дает основания для проведения ОРМ «получение компьютерной информации» в отношении любых компонентов исследуемой компьютерной системы (например, роутера, TV-бокса или смартфона).

В связи с появлением специального ОРМ, направленного на извлечение компьютерной информации, необходимо разграничить понятия «получение компьютерной информации (далее – ПКИ) и «снятие информации с технических каналов связи» (далее – СИТКС).

Так, например, если компьютерная информация будет негласно извлекаться из «компьютерных хранилищ» (имеются в виду различные жесткие диски, карты памяти и т. п.), в которые она была помещена после ее передачи, то данное ОРМ следует рассматривать как получение компьютерной информации. Если же информация, передаваемая с помощью компьютерных устройств (средств связи), будет перехватываться в текущем времени, т. е. в момент ее передачи, то в этом случае необходимо проводить такое ОРМ, «снятие информации с технических каналов связи». Действия по добыванию компьютерной информации, осуществляемые, как правило, гласно, связанные с простейшими формами обращения к компьютерным ресурсам, находящимся у операторов связи или в открытом доступе, либо к устройствам хранения компьютерной информации, полученной в распоряжение субъектов оперативно-розыскной деятельности, не подразумевающие необходимость преодоления определенных препятствий, целесообразно совершать в рамках иных ОРМ (наведение справок, сбор образцов для сравнительного исследования, гласное

[1] Согласно примечанию к ст. 272 УК РФ «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.).

Основной задачей при осуществлении ПКИ является получение копии компьютерной информации, находящейся на машинных носителях информации целевой компьютерной системы.

Общей целью рассматриваемого мероприятия выступает получение оперативно значимой информации об указанных выше объектах ОРМ «получение компьютерной информации», которая реализуется в процессе выявления, предупреждения, пресечения и раскрытия преступлений экстремистской направленности и террористического характера. Конкретная же цель ОРМ «получение компьютерной информации» будет определяться той тактической задачей, которую предполагается решить с его помощью. Например, информация, полученная в ходе проведения указанного ОРМ, может быть использована непосредственно для документирования преступной деятельности лиц, совершающих преступления экстремистской направленности и террористического характера. Помимо этого, целью данного ОРМ может выступать создание условий для успешного осуществления иных ОРМ, которые следует проводить на стадии реализации оперативно-розыскных материалов, например, оперативного эксперимента, проверочной закупки, наблюдения, заканчивающегося задержанием лица (лиц) с поличным.

Содержательная сторона рассматриваемого ОРМ включает в себя конкретные действия, а также тактические приемы получения компьютерной информации. Как уже отмечалось выше, указанное ОРМ относится к категории оперативно-технических мероприятий, поэтому оперуполномоченному подразделения по противодействию экстремизму – инициатору ОРМ важно четко понимать, что может быть отнесено к категории «компьютерная информация».

Согласно ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых государств в борьбе с преступлениями в сфере компьютерной информации под компьютерной информацией следует понимать информацию, находящуюся в па-

мяти компьютера, на машинных или иных носителях в форме, доступной для восприятия ЭВМ, или передающуюся по каналам связи[1].

Категория «компьютер» (компьютерная система[2]) включает в себя разнообразные устройства, предназначенные для автоматизированной обработки оцифрованных данных (персональные компьютеры и сетевые компьютерные устройства, серверы, ноутбуки, сотовые телефоны, смартфоны, планшеты, банкоматы и др., функционирование которых основано на использовании программно-вычислительных систем, предназначенных для автоматизированного ввода, хранения, обработки и передачи данных в цифровой форме).

Под обработкой информации в компьютерных системах понимаются операции по вводу-выводу, передаче, хранению, копированию, модификации и удалению оцифрованных данных, выполняемые по заданным в программном обеспечении алгоритмам.

Перечень носителей компьютерной информации, на которых она может долговременно храниться и с которых может переноситься на компьютер при подключении их к нему, довольно широк. Это могут быть встроенные и внешние накопители на жестких магнитных дисках, карты памяти, оптические диски, CD и DVD-диски и др. Компьютерная информация непродолжительное время может находиться в микросхемах памяти самого компьютера (ОЗУ, ПЗУ, ППЗУ), а также микросхемах управляемого им периферийного оборудования (принтеров, сканеров, факсов и др.). Она может передаваться между компьютерными устройствами по техническим каналам связи в информационно-телекоммуникационных сетях, подвергаясь при этом обработке (оставляя определенные следы) в обеспечивающих передачу промежуточных сетевых устройствах (серверах, маршрутизаторах, концентраторах, модемах и др.).

---

[1] См.: О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации»: федер. закон от 01.10.2008 № 164-ФЗ. URL: http://consultant.ru

[2] Компьютерная система – это набор аппаратных средств и периферийных устройств, составляющих в совокупности вычислительную машину. (См.: Справочник технического переводчика. URL: https://technical_translator_dictionary.academic.ru/93704).

Процесс оцифровки данных заключается в переведении (преобразовании) информации в компьютерную форму, которая в настоящее время в основном ассоциируется с цифровой формой представления данных.

Благодаря постоянному снижению стоимости хранения информации огромные ее массивы могут сохраниться в цифровой форме и использоваться для автоматизированной обработки, что, несомненно, создает особые условия для повышения эффективности оперативно-розыскной деятельности, связанной с информационным поиском.

Получение компьютерной информации может осуществляться:

– при доступе (непосредственном или дистанционном, т.е. через компьютерную сеть) к устройствам памяти, установленным в компьютере и периферийном оборудовании;

– при копировании данных с внешних устройств хранения информации;

– при получении информации с технических каналов связи и входящих в них промежуточных обслуживающих устройств.

Во всех случаях информация может быть получена в виде отдельных текстовых, графических, аудио- и видеодокументов либо выборок по заданным условиям из специализированных баз данных (файлы и распечатки).

Основу ОРМ «получение компьютерной информации» составляют достаточно сложные в техническом плане и требующие специальной подготовки действия, направленные на добывание хранящейся в компьютерных системах или передаваемой по каналам связи информации о лицах, событиях и фактах, вызывающих оперативный интерес[1].

К участию в проведении ОРМ, связанных с получением компьютерной информации, необходимо привлекать соответствующих специалистов. Часть 4 ст. 6 Закона об ОРД предусматривает использование оперативно-технических сил и средств подразделений Федеральной службы безопасности, органов внутренних дел в порядке,

[1] См.: *Осипенко А. Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. 2016. № 3. С. 85.

определенном в межведомственных нормативных актах или соглашениях между органами, осуществляющими оперативно-розыскную деятельность. Из данной нормы также следует, что субъектами ОРМ «получение компьютерной информации» выступают:

– оперативные сотрудники подразделений по противодействию экстремизму – инициаторы проведения ОРМ;

– сотрудники подразделений специальных технических мероприятий, являющиеся исполнителями ОРМ.

Для определения конкретных действий, способных обеспечить получение компьютерной информации в рамках рассматриваемого ОРМ, необходимо выделить возможные источники оперативно значимых компьютерных данных. Условно они могут быть разделены на виды, для каждого из которых характерна своя специфика получения компьютерных данных:

1) технические источники оперативно значимой информации;

2) информационные ресурсы сети Интернет;

3) сетевые каналы коммуникации;

4) базы данных, формируемые в информационных системах государственных органов и коммерческих структур, в том числе банков и операторов связи.

К техническим источникам оперативно значимой информации можно отнести:

– средства вычислительной техники, включая средства сотовой связи и мобильные устройства, обеспечивающие доступ к сетевым ресурсам, содержащие сведения о лицах подготавливающих, совершающих либо совершивших преступления экстремистской направленности и террористического характера;

– носители компьютерной информации, на которых могут храниться данные, представляющие оперативный интерес;

– устройства, фиксирующие компьютерные данные, поступающие от различных датчиков (радиочастотных идентификаторов, GPS-трекеров, нательных датчиков, передающих физиологические показатели и сведения о местоположении, и т. п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации;

– сетевое оборудование, через которое осуществляются коммуникационные акты лиц, подготавливающих, совершающих либо совершивших преступления экстремистской направленности и террористического характера.

Среди информационных ресурсов сети Интернет, обследование которых позволяет получить компьютерную информацию, **выделяют:**

– информационные ресурсы, содержащие сведения о совершении преступлений экстремистской направленности и террористического характера, а также о лицах, их совершающих (сайты экстремистских и террористических организаций, при помощи которых распространяются экстремистские материалы и публичные призывы к осуществлению экстремистской и террористической деятельности, ведется пропаганда идей экстремизма и терроризма, демонстрируется атрибутика или символика экстремистских и террористических организаций либо нацистская атрибутика или символика, вовлекаются и вербуются новые участники, проводится их обучение, осуществляется планирование и координация экстремистской и террористической деятельности, и т. п.);

– места сетевого общения радикальных нацистов и криминально настроенных лиц (закрытые сайты, сетевые форумы и чаты, сообщества экстремистской и террористической направленности в социальных сетях и др.) и их персональные страницы в социальных сетях.

Информация в сети Интернет может быть представлена в виде следов противоправной деятельности, ссылок на материалы, запрещенные к распространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений экстремистской направленности и террористического характера.

К источникам получения компьютерной информации в первую очередь относятся сетевые каналы коммуникации, задействованные экстремистами и террористами для координации своих действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и т.п. Обнаружение и контроль таких каналов обеспечивают оперативным подразделениям существенные преимущества. При этом важно учиты-

вать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интернет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegram и др.), причем многие из них представляют услуги шифрования передаваемых данных.

Оперативно значимая информация может быть получена и из таких источников, как выборки, генерируемые по заданным условиям при анализе сведений из различных **баз данных, формируемых в информационных системах** государственных органов и коммерческих структур, в том числе банков и операторов связи. Например, информацию, размещенную на серверах в Интернете, можно получить у провайдера интернет-услуги либо через организации, предоставляющие услуги хостинга.

С позиции оперативно-розыскной науки и практики содержание ОРМ «получение компьютерной информации» связано с применением особых способов доступа к информационным ресурсам и источникам, содержащимся в компьютерных системах. К таким способам, в частности, могут быть отнесены:

1. Негласное применение специального программного обеспечения и оборудования для скрытого съема данных с компьютерных устройств, потенциально содержащих оперативно значимую информацию, включая несанкционированный дистанционный доступ к компьютерным устройствам, имеющим сетевое подключение.

2. Оперативно-розыскной мониторинг представляющих оперативный интерес сетевых информационных ресурсов, реализуемый через: автоматизированный поиск ресурсов, содержащих запрещенную к распространению информацию; оперативно-розыскное изучение материалов выявленных ресурсов, связанных с деятельностью экстремистских или террористических организаций (сообществ); наблюдение за закрытыми для общего доступа местами сетевого общения экстремистской направленности.

3. Негласная установка специального программного обеспечения в компьютерные устройства лиц, подозреваемых в осуществлении экстремистской или террористической деятельности, которое позволяет фиксировать содержание осуществляемых с этих компьютеров сеансов связи. При этом формирование файлов с информа-

цией о содержании таких сеансов, скрытно направляемых на определенный сетевой адрес, происходит на обозначенном компьютере, в отличие от ОРМ «снятие информации с технических каналов связи», где информация снимается с каналов связи в процессе ее передачи с использованием предоставляемой оператором связи возможности подключения к указанным каналам.

4. Применение аналитического программного обеспечения для выявления оперативно значимой информации в базах данных различного назначения. Указанный способ получения доступа к информационным ресурсам и источникам отражен в ст. 2 упомянутого выше Федерального закона от 6 июля 2016 г. № 374-ФЗ, которая дополнила ст. 15 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности» ч. 4, закрепившей право федерального органа исполнительной власти в области обеспечения безопасности получать на безвозмездной основе от государственных органов и внебюджетных фондов информационные системы и (или) базы данных, необходимые для выполнения возложенных на него обязанностей, в том числе путем получения удаленного доступа к ним.

5. Негласный или гласный осмотр компьютеров, мобильных телефонов, планшетов и других устройств, при котором хранение данных сопровождается копированием компьютерной информации[1].

В соответствии с ч. 2 ст. 8 Закона об ОРД получение компьютерной информации является ОРМ, ограничивающим конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища. Его проведение допускается на основании судебного решения и при наличии информации, указанной в пп. 1–3 комментируемой части статьи Закона об ОРД. Эта же статья закрепляет возможность получения компьютерной информации без судебного решения по основаниям, предусмотренным п. 5 ч. 2 ст. 7 Закон об ОРД.

[1] См.: Осипенко А. Л. Указ. соч. С. 87.

2. ПОРЯДОК ПОДГОТОВКИ И ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Ввиду отсутствия в оперативно-розыскном законодательстве и ведомственных нормативных правовых актах развернутого перечня действий, допустимых при осуществлении ОРМ «получение компьютерной информации», считаем возможным предложить авторский алгоритм реализации данного мероприятия при выявлении, предупреждении, пресечении и раскрытии преступлений экстремистской направленности и террористического характера.

Структурно проведение ОРМ «получение компьютерной информации» состоит из нескольких этапов:

1. Подготовительный (оценка сложившейся оперативно-тактической ситуации, послужившей основанием для принятия решения о проведении ОРМ; определение субъекта ПКИ; согласование проведения ОРМ с учетом реальных технических возможностей оперативно-технического подразделения; определение объема времени, которое отводится на осуществление мероприятия; получение судебного решения на проведение ОРМ; сбор дополнительных сведений об исследуемой системе; подготовка задания на проведение ОРМ; подбор технических средств для негласного получения информации).

2. Рабочий (непосредственное проведение ОРМ «получение компьютерной информации»).

3. Заключительный (документальное оформление результатов проведенного ОРМ).

На подготовительном этапе оперативный сотрудник при наличии информации, указанной в пп. 1–3 ч. 2 ст. 8 Закона об ОРД[1], выносит мотивированное постановление о возбуждении перед судом ходатайства о проведении ОРМ «получение компьютерной инфор-

[1] Основания для проведения ОРМ «получение компьютерной информации»: а) признаки подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; б) лица, подготавливающие, совершающие или совершившие противоправное деяние, по которому производство предварительного следствия обязательно; в) события или действия (бездействие), создающие угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

мации» и утверждает его у одного из руководителей органа, осуществляющего оперативно-розыскную деятельность. Согласно ч. 3 ст. 9 Закона об ОРД перечень категорий таких руководителей устанавливается ведомственными нормативными актами.

Получение компьютерной информации может носить гласный и негласный характер. В первом случае данное ОРМ осуществляется только с согласия владельцев исследуемых объектов, которое дается в письменной форме.

Проведение ОРМ «получение компьютерной информации», которое ограничивает конституционные права человека и гражданина, отраженные ч. 1 ст. 9 ФЗ об ОРД, допускается только на основании судебного решения.

В связи с этим соответствующие руководители вправе обращаться в суд за разрешением на проведение ОРМ «получение компьютерной информации» по месту его проведения или месту нахождения органа, ходатайствующего об его проведении.

Указанные материалы рассматриваются уполномоченным на то судьей единолично, если законодательством Российской Федерации не установлен иной порядок их рассмотрения, и незамедлительно. Суд (судья) не вправе отказать в рассмотрении таких материалов в случае их представления.

Основанием для решения судьей вопроса о проведении ОРМ является мотивированное постановление одного из руководителей органа, осуществляющего оперативно-розыскную деятельность.

По требованию судьи ему могут представляться также иные материалы, подтверждающие необходимость проведения ОРМ «получение компьютерной информации», за исключением сведений о лицах, внедренных в организованные преступные группы, штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и тактике проведения ОРМ.

По результатам рассмотрения материалов, содержащих основания для проведения ОРМ «получение компьютерной информации», судья разрешает либо отказывает в его проведении, о чем выносит

мотивированное постановление, которое заверяется гербовой печатью и выдается инициатору проведения ОРМ вместе с представленными им материалами.

Срок действия такого постановления исчисляется сутками со дня его вынесения и не может превышать шести месяцев, если иное не указано в самом постановлении. При этом течение срока действия постановления не прерывается. Если возникает необходимость в продлении срока действия постановления, то судья может вынести соответствующее судебное решение только на основании вновь представленных материалов.

В случае, если судья, рассмотрев представленные материалы, посчитал их недостаточными для принятия решения об ограничении конституционных прав человека и гражданина, указанных в ч. 1 ст. 9 Закона об ОРД, и отказал в проведении ОРМ, орган, осуществляющий оперативно-розыскную деятельность, вправе обратиться по этому же вопросу в вышестоящий суд.

В ситуациях, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение ОРМ «получение компьютерной информации» с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала ОРМ орган, его осуществляющий, обязан получить судебное решение о проведении такого мероприятия либо прекратить его проведение.

Проведение ОРМ «получение компьютерной информации» без судебного решения, согласно ч. 10 ст. 8 Закона об ОРД, допускается в случае:

принятия решения об обеспечении безопасности органов, осуществляющих оперативно-розыскную деятельность;

обеспечения безопасности должностных лиц органов, осуществляющих оперативно-розыскную деятельность, при наличии письменного согласия указанных лиц.

Ввиду отсутствия в действующем оперативно-розыскном законодательстве четкого понимания природы компьютерной информации и неурегулированности в законе вопроса о том, в каких случаях ее получение ограничивает конституционные права человека и гражданина, указанные в ч. 2 ст. 8 Закона об ОРД, а при каких условиях данная информация не подлежит защите с помощью судебного контроля, считаем, что во всех без исключения ситуациях проведение данного ОРМ требует судебного решения. И пока не наработана практика использования в доказывании результатов нового ОРМ, именно такой механизм будет обеспечивать защиту от нивелирования их доказательственного значения.

Получив судебное решение, инициатор проведения ОРМ, связанного с получением компьютерной информации, заполняет бланк задания и через руководителя органа, осуществляющего оперативно-розыскную деятельность, направляет его в порядке, определенном межведомственными нормативными актами или соглашениями между подразделениями, осуществляющими оперативно-розыскную деятельность, в оперативно-техническое подразделение органов внутренних дел или Федеральной службы безопасности.

Задание на проведение ОРМ «получение компьютерной информации» имеет типовую форму, аналогичную той, которая заполняется при проведении СИТКС, ПТП и иных организационно-технических мероприятий. Заполнение задания осуществляется с учетом методических рекомендаций подразделений, обеспечивающих проведение специальных технических мероприятий.

В задании на проведение ОРМ «получение компьютерной информации» инициатором указываются дата вынесения постановления судьи, наименование суда, фамилия и инициалы судьи, давшего разрешение на осуществление.

Должностные лица, утвердившие постановление и подписавшие задание на проведение ОРМ «получение компьютерной информации», несут персональную ответственность за достоверность изложенных в них данных, законность и обоснованность проведения самого мероприятия в соответствии с законодательством Российской Федерации.

Если проведение ПКИ невозможно (либо стало невозможным) в силу объективных причин, то инициатор ОРМ ставится об этом в

известность, а на бланке задания делается запись с указанием конкретной причины его невыполнения, которая заверяется подписью должностного лица – исполнителя ПКИ.

Судебные решения на право проведения ОРМ «получение компьютерной информации» и материалы, послужившие основанием для его принятия, хранятся только в оперативном подразделении, инициировавшем его проведение.

Рабочим этапом является непосредственное проведение мероприятия, которое предполагает получение данных от любого компонента компьютерной системы.

При проведении ОРМ «получение компьютерной информации» с компьютерных систем и электронных носителей информации обеспечивается решение следующих задач:

– определение состояния (работоспособности) компьютерной системы (носителя информации), типа, производителя, модели и иных технических характеристик, относящиеся к компьютерной системе (носителю информации);

– создание побитового образа электронных носителей информации;

– извлечение с накопителей (на жестких магнитных дисках, картах памяти) оперативно значимых сведений, таких как фотографии, видеоизображения, звуковые файлы, текстовая информация;

– извлечение контактной информации и электронной переписки;

– восстановление удаленных или частично поврежденных данных;

– исследование закодированных файлов;

– выявление и уточнение назначения программ управления аппаратными средствами, подключаемыми и используемыми с представленным средством вычислительной техники;

– изучение протоколов работы пользователя (или программ) на компьютерной технике и интерпретация их действий.

В настоящее время дать подробное описание всех особенностей практического осуществления ОРМ «получение компьютерной информации» не представляется возможным, поскольку, как уже отмечалось ранее, отсутствует нормативное толкование его содержания,

а практика применения данного мероприятия еще не наработана в достаточном объеме.

На завершающем этапе ОРМ «получение компьютерной информации» осуществляется документальное оформление процесса его проведения и полученных при этом данных.

Результаты ОРМ «получение компьютерной информации» могут оформляться в виде оперативно-служебных документов (справок, сводок), аналогичных тем, которые оформляются по результатам проведения СИТКС, электронного досмотра и иных ОТМ, с приложением информации на электронных (машинных) носителях, исключающих утрату хранящихся на них сведений. Иными словами, в результате проведения ОРМ «получение компьютерной информации» должен быть получен «документ на машинном носителе», т.е. созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Следует отметить, что отчуждаемые носители информации (оптические носители, внешние накопители на магнитных или твердотельных дисках, карты памяти и сим-карты) могут быть использованы не только как средства для документирования информации, получаемой в ходе проведения ОРМ «получение компьютерной информации», и устройствами для запуска в исследуемой компьютерной системе операционных систем, предназначенных для криминалистического анализа (Forensic Tools), но и сами, являясь компонентами исследуемой компьютерной системы, часто выступают источниками важной доказательственной информации.

Поэтому в зависимости от сложившейся практики взаимодействия с подразделениями специальных технических мероприятий, возможно составление и направление в Бюро специальных технических мероприятий соответствующих запросов на сохранение носителей информации, результатов проведенного ОТМ, которые могут быть использованы в качестве доказательств.

ЗАКЛЮЧЕНИЕ

На сегодняшний день ввиду развития информационных технологий и повсеместной информатизации общества, деятельность представителей экстремистских и террористических организаций осуществляется посредством обмена данными в сети Интернет. Массовая доступность глобальной Сети создает благоприятные условия для совершения преступлений экстремистской направленности и террористического характера в виртуальном пространстве. Именно в нем экстремисты и террористы получают недопустимую в реальном обществе свободу деятельности и становятся не только потребителями интернет-ресурсов, но и создателями экстремистских сайтов, форумов, блогов. В свою очередь, противодействуя экстремизму и терроризму, сотрудники оперативных подразделений вынуждены подстраиваться под формирующуюся конъюнктуру преступности и находить новые способы получения информации. Одним из таких способов стало ОРМ «получение компьютерной информации».

В методических рекомендациях представлен единый алгоритм реализации ОРМ «получение компьютерной информации» при выявлении, предупреждении, пресечении и раскрытии преступлений экстремистской направленности и террористического характера.

Предложенный алгоритм направлен на повышение эффективности и результативности оперативно-служебной деятельности сотрудников подразделений по противодействию экстремизму и призван способствовать активизации и оптимизации борьбы с преступностью в рассматриваемой сфере.

Оглавление

Учебное издание

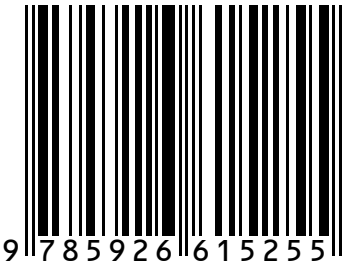
АЛГОРИТМ РЕАЛИЗАЦИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» ПРИ ВЫЯВЛЕНИИ, ПРЕДУПРЕЖДЕНИИ, ПРЕСЕЧЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА

Методические рекомендации

Составители:
Осипенко Анатолий Леонидович
Белый Андрей Григорьевич
Стукалов Вячеслав Владимирович
Запорожец Екатерина Владимировна
Голяндин Николай Петрович
Гуров Данил Валерьевич
Мещерин Александр Иванович

Редактор *И. А. Мосенцева*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1525-5



Подписано в печать 08.02.2019. Формат 60x84 1/16.
Усл. печ. л. 1,4. Тираж 70 экз. Заказ 766.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.