ВОПРОСЫ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ МВД РОССИИ НЕПРАВОМЕРНЫМ ОПЕРАТИВНО-РОЗЫСКНЫМ МЕРОПРИЯТИЯМ ПРИ ПОДГОТОВКЕ И ПРОВЕДЕНИИ ПУБЛИЧНЫХ МЕРОПРИЯТИЙ

УДК 343.3

Комаров Валерий Валентинович
кандидат юридических наук
доцент кафедры деятельности органов внутренних дел в особых условиях
Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя
г. Москва, Российская Федерация
84991912028@mail.ru

Комарова Татьяна Егоровна
начальник группы Главного управления охраны общественного порядка Федеральной службы войск национальной гвардии Российской Федерации
г. Москва, Российская Федерация
dr.rosgvard@yandex.ru

Тараканова Татьяна Эдуардовна
курсант факультета подготовки специалистов в области информационной безопасности
Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя
г. Москва, Российская Федерация
tatyana2016sport@yandex.ru

Для цитирования:
Комаров В.В., Комарова Т.Е., Тараканова Т.Э. Вопросы организации противодействия МВД России неправомерным оперативно-розыскным мероприятиям при подготовке и проведении публичных мероприятий // Вестник Санкт-Петербургского военного института войск национальной гвардии. 2020. № 1 (10). С. 98–104. URL: http: //vestnik-spvi.ru/2020/03/022.pdf

Аннотация. В статье изучены методы получения информации и применение специальных технических средств для негласного получения информации преступниками при подготовке, планировании и совершении преступлений. При рассмотрении вопросов, касающихся законодательства в области оборота специальных технических средств для негласного получения информации, предлагаются конкретные изменения в целях обеспечения интересов индивидуума (гражданина), коллектива, общества и государства.

Ключевые слова: охрана общественного порядка, публичные мероприятия, технические средства, информационные технологии правонарушения, акции протеста.

В последнее время при проведении публичных массовых мероприятий в Российской Федерации (особенно несогласованных) все чаще констатируется их организованность и тенденции к использованию «реализации права на свободу слова» для совершения противоправных действий. При этом отмечается высокий уровень технической оснащенности правонарушителей.

Так, в июле – сентябре 2019 года в Москве прошли масштабные акции протеста с политическими требованиями, поводом для которых послужил отказ в регистрации ряду оппозиционных кандидатов на выборах в Мосгордуму. Изначально ключевым требованием протестующих был допуск к выборам независимых от власти кандидатов. Однако позднее стали появляться требования роспуска Московской городской избирательной комиссии в целом и смены власти в стране.

Было отказано всем кандидатам из команд Навального, Гудкова, большинству кандидатов от партии «Яблоко»

ЮРИДИЧЕСКИЕ НАУКИ

ISSN 2587-7402 (онлайн)
http: //vestnik-spvi.ru

Масштабные протестные мероприятия состоялись 14 июля (акция позиционировалась в формате встречи с гражданами, что по мнению организаторов не требовало согласования, соответствующее уведомление в органы исполнительной власти не подавалось), 20 июля согласованное мероприятие с участием до 12 тыс. человек, 27 июля в несогласованной (уведомление не подавалось) акции приняло участие до 3500 человек, 3 августа в несогласованной (уведомление не подавалось) акции приняло участие до 3500 человек.

Наиболее многочисленным до 20 тысяч участников стал согласованный митинг, прошедший 10 августа на проспекте Академика Сахарова, после которого в центральной части города Москвы была проведена несогласованная публичная акция.

Проведенные акции характеризовались созданием помех функционированию объектов транспортной и социальной инфраструктуры, перекрытием движения пешеходов и доступа граждан к жилым помещениям, массовыми выходами на проезжую часть с созданием помех движению автотранспорта, активным неповиновением сотрудникам полиции и Росгвардии, неоднократными попытками прорыва оцепления, оказанием сопротивления задержанию, а также скандированием оскорбительных лозунгов в адрес высших органов государственной власти и правоохранительных органов.

Отмечался высокий уровень организованности и мобильности участников указанных протестных мероприятий, сопровождающийся новейшими приемами оповещения с применением инновационного технического сопровождения.

В данной статье мы рассмотрим лишь некоторые вопросы совершенствования противодействия этим проявлениям на ранней стадии.

Отметим, что в связи с появившимися в последнее время услугами трансграничной торговли, которые имеют несовершенное таможенное регулирование, в руках злоумышленников появляются устройства, предназначенные для негласного получения информации.

Так, при организации групповых нарушений общественного порядка в июле - августе 2019 года в г. Москве правонарушители использовали для общения между собой специальный зашифрованный мессенджер «*Confide*». Отправка сообщения проста – выбираем абонента, вводим сообщение, если необходимо прикладываем изображение и жмем отправить. Так как мессенджер не столь популярен, как настоящие популярные мессенджеры, и учитывая специфику его использования, разработчики включили звуковое оповещение о прочтении вашего сообщения абонентом.

В этой части помимо непривычного интерфейса других особенностей нет. Рассмотрим,

14 июля в акции приняло участие до 1000 человек, задержано и доставлено в ОВД 33 лица, составлено 29 протоколов об административном правонарушении.

20 июля на согласованном мероприятии с участием до 12 тыс. человек задержан и доставлен в ОВД один человек, в отношении которого составлен протокол об административном правонарушении.

27 июля в несогласованной акции приняло участие до 3500 человек, задержан 1431 человек, составлено 1225 протоколов об административном правонарушении.

3 августа в несогласованной акции приняло участие до 3500 человек, задержан 941 человек, составлено 922 протокола об административном правонарушении.

10 августа на проспекте Академика Сахарова проведена несогласованная публичная акция, задержано за различные правонарушения 229 человек, составлено 210 протоколов об административном правонарушении.

как все это выглядит со стороны получателя сообщения. Получив сообщение, можно увидеть на экране набор полосочек, каждое отдельное слово – одна полоска. Чтобы прочитать их, нужно провести пальцем сверху вниз по строкам. Наименование абонента при этом с экрана исчезает. Строки будут открываться по одной, таким образом увидеть сразу весь текст одновременно невозможно. Пока вы не нажали кнопку назад, вы можете просматривать построчно сообщение сколько угодно.

Если вам направили картинку, просмотреть ее тоже можно только по частям, как раз шириной в один условный палец.

После того, как вы прочитали сообщение, и нажимаете кнопку «назад», оно полностью уничтожается. Нет никаких историй переписки, логфайлов. Сообщение исчезает полностью, не оставляя следов.

Кроме того, использовались рации китайской фирмы *Puxing*, принимающие в *UHF* и *VHF* диапазонах, передающих, правда, только в *UHF*. Данные рации находятся в открытом доступе в сети Интернет.

Преступники переделывают рацию. Один штекер засовывают в гнездо гарнитуры, второй – в микрофон, выставляют громкость на гарнитуре, и уровень микрофона на компьютере и начинают записывать.

Данное устройство позволяет прослушивать

разговоры сотрудников правоохранительных органов, узнавать их намерения, слушать онлайн «Разговоры сотрудников полиции по радиостанции», что позволяет правонарушителям своевременно корректировать свои действия и скрывать следы преступления.

Нарушение оборота специальных технических средств, предназначенных для негласного получения информации, попадает под уголовную ответственность статьи 138.1 Уголовного кодекса Российской Федерации (УК РФ). Данное преступление относится к преступлениям против Конституционных прав и свобод человека и гражданина, т. е. предполагается защита от незаконного собирания информации о частной жизни, но это регламентируется ст. 137 УК РФ, защита тайны переписки регламентируется ст. 138 УК РФ, возникает вопрос правильно ли трактуется данная статья и к какому виду преступлений относится.

Если рассмотреть субъективную сторону данного преступления, то она характеризуется виной в виде прямого умысла. Доказывание данного умысла является проблемой для правоохранительных органов, потому что не всегда злоумышленники правдиво рассказывают о своих истинных намерениях.

Свободный доступ к сайтам, где можно приобрести специальное техническое средство для негласного получения информации провоцирует преступников на использование данных средств в своей деятельности.

Вместе с тем, Постановление Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина», дающее разъяснения касательно статьи 138.1 УК РФ, что еще больше «развязывает руки» потенциальным злоумышленникам и торговцам «шпионскими гаджетами».

В постановлении Верховного Суда Российской Федерации разъясняется, что участие в незаконном обороте специальных технических средств не может свидетельствовать о виновности лица в совершении преступления, предусмотренного статьей 138.1 УК РФ, если его умысел не был направлен на приобретение и (или) сбыт именно таких средств.

Действия лица с намерением использовать техническое средство, например, в целях обеспечения личной безопасности, и не предполагающие применять его в качестве средства посягательства на конституционные права граждан, не могут быть расценены как нарушение законодательства [1].

Благодаря этому Постановлению, границы, регламентирующие использование специальных технических средств, для негласного получения информации, стали больше размыты, и злоумышленники получили возможность уйти от уголовной ответственности. Поэтому законодательство в области незаконного оборота специальных технических средств, предназначенных для негласного получения информации, требует более детального изучения и совершенствования с учетом судебной практики.

В Российском законодательстве под специальными техническими средствами, предназначенными для негласного получения информации, понимаются приборы, системы, комплексы, устройства, специальные инструменты, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя [2].

К специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, с открыто расположенными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя [2].

Ввоз и вывоз в Российскую Федерацию специальных технических средств осуществляется по лицензиям [3]. В соответствии со ст. 6 Федерального закона Российской Федерации «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ запрещается проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных для негласного получения информации, не уполномоченными на то настоящим законом физическими и юридическими лицами (ст. 6 Федерального закона Российской Федерации «Об оперативно-розыскной деятельности») [4].

На наш взгляд, для конкретизации законодательной базы, необходимо внести дополнения в п. 9 Перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности (утверждено постановлением Правительства Российской Федерации от 1 июля 1996 г. № 770) которые будут регламентировать список утвержденных технических устройств, характеристики технических устройств, границы использования этих устройств [5].

Отдельный пункт подзаконного акта (Постановление Правительства Российской Федерации от 10 марта 2000 г. № 214) обязывает граждан уведомлять правоохранительные органы или другие регулирующие организации о намерении применения или использования таких технических средств, и в каких целях, чтобы избежать привлечения к уголовной ответственности [3].

Предлагаем более подробно рассмотреть современные формы противодействия незаконному обороту специальных технических средств. Оперативные подразделения проводят ряд оперативных мероприятий по обнаружению и предотвращению незаконного оборота специальных технических средств.

В целях получения информации о злоумышленнике, о его общении в социальных сетях, используется специальное оперативно-розыскное мероприятие (ОРМ) – наведение справок в сети интернет. В рамках указанного ОРМ осуществляется сбор информации о злоумышленнике из открытых источников в сети интернет. Наводятся справки о лице, его жизни, родственных и дружеских связях, наличии недвижимого имущества, регистрации по месту жительства, судимости, выдаче документов, удостоверяющих личность и служебных удостоверений, наличии оружия и др.

В настоящее время в открытом доступе имеется большое количество программ, которые помогают найти информацию о человеке в сети Интернет.

Например, *SocialMapper* – это инструмент с открытым исходным кодом, который использует распознавание лиц для корреляции профилей социальных сетей на разных сайтах в больших масштабах. Программа использует автоматизированный подход для поиска в популярных сайтах социальных сетей по именам и изображениям целей, чтобы точно определять и группировать присутствие человека, выводя результаты в наглядный отчёт, который оператор-человек может быстро просмотреть.

Если рассмотреть практическое применение для правоохранительных органов, в рамках «наведения справок», то данная программа выдает в результате страницы пользователей, которые когда-либо выкладывали фотографии с интересующим нас человеком, то есть можно изучить родственные, дружеские, либо преступные связи. *SocialMapper* поддерживает следующие платформы социальных сетей: *LinkedIn, Facebook, Twitter, GooglePlus, Instagram, VKontakte, Weibo, Douban.*

SpiderFoot обрабатывает одновременно более 100 открытых источников, доступна расширенная настройка. Также есть фильтр по кейсам: поиск всевозможного о человеке, поиск цифровых следов с помощью поисковых роботов и поисковиков, черные списки и другие открытые источники для проверки на вредоносность и сбора информации. Последний лучше всего подходит для расследования.

Таким образом, в качестве средств ОРМ «Наведение справок» на основе анализа открытых источников в сети Интернет должны использоваться специальные программы поиска и анализа данных. Для удобства изучения материала и технологий, применяемых в открытых источников в сети Интернет, мы рассмотрели некоторые инструменты сбора информации в сети Интернет. На сегодняшний день всё больше распространяется *SOCMINT* (сбор сведений из социальных сетей) – это подраздел открытых источников в сети Интернет, фокусирующийся на сборе и мониторинге данных в социальных сетях. Так как сейчас почти не осталось людей, которые не зарегистрированы ни в одной социальной сети.

В случаях, когда необходимо использование информационных технологий в целях получения информации с телефона, получение данных о сообщениях, программах, которые были удалены необходимо использовать ОРМ.

Исследование компьютера нужно осуществлять путем восстановления и изучения файлов, хранившихся на компьютере или телефоне.

Программа *R-Studio* – это семейство утилит для восстановления файлов. Программное обеспечение работает как на локальном, так и на удаленном компьютере в Сети, даже если разделы отформатированы, повреждены или удалены. Уникальная технология сканера *Intelligentscan* и простой в использовании пользовательский интерфейс позволяют полностью контролировать процесс восстановления данных.

Программа осуществляет:

- Побайтное копирование любого объекта панели Диски, а также копирование разделов и жестких дисков.

- Восстановление файлов с поврежденных или удаленных разделов, сжатых файлов, зашифрованных файлов.

- Поддержка дедупликации.

- Поддержка Символических ссылок. Опция по восстановлению симлинков в Технической версии.

- Поддержка обработки журналов для файловых систем.

- Поддержка обработки журналов мягких апдейтов для файловой системы *UFS*.

- Поддержка расширенных атрибутов для файловых систем.

- Поддержка сжатых файлов на файловой системе.

- Распознавание локализованных имен.

- Восстановленные файлы могут быть сохранены на любой, включая сетевой, диск доступный локальной операционной системой.

После успешной проверки программа отобразит все содержимое, которое ранее находи-

лось по заданному пути в выбранном разделе. Красным крестом отмечены те файлы и папки, которые были удалены. Чтобы восстановить их, необходимо поставить галочку напротив того элемента, который необходимо восстановить и нажать на «Восстановить помеченные данные».

Также данная программа сканирует удаленный хост. В новой сетевой версии *R-Studio* данные анализируются на удаленном хосте вместо предварительной загрузки на локальный хост, что резко увеличивает скорость процедуры восстановления с удаленного компьютера. Информацию о сканировании можно сохранить на локальном или удаленном компьютере. При восстановлении данных по сети на удаленном компьютере восстановленные файлы могут быть сохранены на другом устройстве или на том же компьютере. Это полезно, когда удаленный компьютер имеет рабочий диск (например, внешний USB-накопитель), и вам не нужно передавать файлы по сети.

Получение компьютерной информации необходимо проводить с помощью программного обеспечения – *BelkasoftEvidenceCenterUltimate*.

BelkasoftEvidenceCenter облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. Программа быстро извлечёт цифровые улики из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий iOS, Blackberry и Android, *UFED, JTAG* и *chip-off* дампов.

EvidenceCenter автоматически проанализирует источник данных и представит наиболее значительные улики для обзора, подробного изучения или включения в отчёт. Ищет скрытую и зашифрованную информацию, ищет в необычных местах, извлекает удаленные и поврежденные данные с помощью карвинга, исследует файлы малоизвестных форматов для нахождения еще большего числа улик. Поиск включает неразмеченные и неиспользуемые области, *$MFT, $Log, VolumeShadowCopy* и другие специальные и малоизвестные области операционной системы.

Изучая мобильные телефоны необходимо использовать устройство криминалистического исследования сотовых телефонов «*UFED*». Данное устройство может быстро и безопасно извлекать данные из мобильных телефонов. Можно получить данные о телефонной книге, текстовых сообщениях, фотографиях, звуковых файлов и др.

Таким образом, указанные программы используются правоохранительными органами в настоящее время при осуществлении следственных действий и ОРМ.

При киберпреступлениях и атаках средства защиты должны работать быстро и эффективно, чтобы сократить потери. Для этого необходимо использовать указанные нами выше методы компьютерной разведки.

За последние несколько лет в России набирают обороты электронные торговые площадки из Китая, огромный ассортимент и бесплатная доставка, вот что в первую очередь привлекает покупателя. Но у столь успешного проекта есть обратная сторона. По всей стране заведено тысячи уголовных дел за попытку купить: детские игрушки с видеокамерой, разного рода видеоняни, наручные часы с камерой, ручки, очки и т. д. Оборот таких «гаджетов» в российской законодательной плоскости попадает под уголовную ответственность. Преступники используют указанные средства в целях планирования и подготовке к преступлениям.

В данной статье мы рассмотрели вопросы, касающиеся законодательства в области оборота специальных технических средств для негласного получения информации, были предложены конкретные изменения в законодательство, а именно:

- дополнения в п. 9 Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, которые будут регламентировать список утвержденных технических устройств, характеристики технических устройств, границы использования этих устройств [5];

- дополнение в Постановление Правительства РФ от 10 марта 2000 г. № 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» об обязанности граждан уведомлять правоохранительные органы или другие регулирующие организации о намерении применения или использования таких технических средств, и в каких целях, чтобы избежать привлечения к уголовной ответственности.

Также были изучены методы получения информации и применение специальных технических средств для негласного получения информации преступниками при подготовке, планировании и совершении преступлений.

В статье рассмотрены некоторые виды ОРМ, которые помогут для обнаружения специальных технических средств, такие как снятие информации с технических каналов связи; получение компьютерной информации.

Были отражены предложения по использованию программного обеспечения и методах в целях раскрытия преступления, такие как: информация из открытых источников в сети интернет

(*OSINT*), *R-Studio, BelkasoftEvidenceCenterUltimate*, устройство криминалистического исследования сотовых телефонов «*UFED*».

В условиях высокой информатизации, компьютерная разведка является решением задач оперативно-розыскной деятельности при противодействии преступлениям в сфере информационных технологий и киберпространстве.

Таким образом, технический век позволяет говорить о том, что в условиях, когда большинство правонарушений совершается с применением различных современных специальных технических средств, которые не допускается иметь даже на вооружении у правоохранительных органов, рассматриваемый вопрос становится весьма актуальным.

Проведение несогласованных публичных мероприятий, а впоследствии и массовых беспорядков, затрагивает не только интересы индивидуума (гражданина), коллектива, но и в целом интересы общества и государства.

В этой связи необходимы изменения в действующие нормативные правовые акты Российской Федерации в целях дальнейшего применения в борьбе с правонарушениями, в том числе при организации обеспечения охраны общественного порядка при проведении публичных мероприятий.

ЛИТЕРАТУРА

1. Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СудАкт: Судебные и нормативные акты РФ [Электронный ресурс]. URL: https://sudact.ru/law/postanovlenie-plenuma-verkhovnogo-suda-rf-ot-25122018/ (дата обращения: 15.02.2020).

2. Федеральный закон от 2 августа 2019 г. № 308-ФЗ «О внесении изменения в статью 138.1 Уголовного кодекса Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4467.

3. Постановление Правительства Российской Федерации от 10 марта 2000 г. № 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» (ред. от 20.03.2018) // Собрание законодательства Российской Федерации. 2000. № 12. Ст. 1292.

4. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (в ред. от 02.08.2019) // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

5. Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности» (в ред. от 15.07.2002) // Собрание законодательства Российской Федерации. 1996. № 28. Ст. 3382.

ISSUES OF ORGANIZATION OF COUNTERACTION TO THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA TO UNLAWFUL OPERATIONAL-SEARCH MEASURES DURING THE PREPARATION AND CONDUCT OF GROUP VIOLATIONS OF PUBLIC ORDER

Komarov Valery Valentinovich
PhD in Low (Candidate of Juridical sciences)
Associate Professor of the Department of Internal affairs in special circumstances
Kikot Moscow University of the Ministry of Internal Affairs of Russia
Moscow, Russian Federation
84991912028@mail.ru

Komarova Tatyana Egorovna
Head of the main Department of Public order protection Federal Service of National Guard Troops of the Russian Federation
Moscow, Russian Federation
dr.rosgvard@yandex.ru

Tarakanova Tatyana Eduardovna
cadet of the faculty: Training specialists in the field of information security
Kikot Moscow University of the Ministry of Internal Affairs of Russia
Moscow, Russian Federation
tatyana2016sport@yandex.ru

Abstract. The article studies the methods of obtaining information and the use of special technical means for secretly obtaining information by criminals in the preparation, planning and commission of crimes. When considering issues relating to legislation in the field of the circulation of special technical means for secretly obtaining information, specific changes are proposed in order to ensure the interests of the individual (citizen), the collective, society and the state.

Keywords: public order, public and mass events, offenses, protests, rally.

ISSN 2587-7402 (онлайн)
http: //vestnik-spvi.ru