

Краснодарский университет МВД России

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
VI Международной научно-практической конференции

(24 ноября 2017 г.)

Краснодар
2018

УДК 343
ББК 67.410.212
А43

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Редакционная коллегия:

А. А. Сафронов, кандидат юридических наук, доцент (председатель);
В. В. Стукалов, кандидат юридических наук (заместитель председателя);
А. Э. Добросмыслов (ответственный секретарь);
А. Г. Белый, кандидат юридических наук, доцент;
В. В. Вечера, кандидат юридических наук;
Е. В. Запорожец, кандидат юридических наук;
А. В. Алехин

Актуальные проблемы теории и практики оперативно-розыскной деятельности : материалы VI Междунар. науч.-практ. конф., 24 нояб. 2017 г. / редкол.: А. А. Сафронов, В. В. Стукалов, А. Э. Добросмыслов, А. Г. Белый, В. В. Вечера, Е. В. Запорожец, А. В. Алехин. – Краснодар : Краснодарский университет МВД России, 2018. – 106 с.

ISBN 978-5-9266-1391-6

Представлены доклады и тезисы выступлений участников VI Международной научно-практической конференции, в которых рассматриваются актуальные проблемы теории и практики оперативно-розыскной деятельности на современном этапе.

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

УДК 343
ББК 67.410.212

ISBN 978-5-9266-1391-6

© Краснодарский университет
МВД России, 2018

Акопов Артур Андреевич,
заместитель руководителя следственного отдела
по Усть-Лабинскому району СУ Следственного комитета
Российской Федерации по Краснодарскому краю;
Николаева Илона Игоревна,
общественный помощник следственного отдела
по Усть-Лабинскому району СУ Следственного комитета
Российской Федерации по Краснодарскому краю

Актуальные проблемы взаимодействия следователя и оперативных сотрудников в ходе уголовного судопроизводства

Предварительное расследование преступлений играет немаловажную роль в уголовном судопроизводстве, так как именно от качества, полноты и степени ответственности, с которой проведена работа на данной стадии уголовного процесса, зависит дальнейшая судьба уголовного дела о совершении того или иного общественно опасного деяния и будет ли привлечено к ответственности виновное лицо или лица.

На эффективности раскрытия, расследования и предупреждения преступлений напрямую сказывается скоординированная и четко налаженная работа органов следствия и органов, осуществляющих оперативно-розыскную деятельность.

И сегодня мы бы хотели подробнее разобрать проблемы, возникающие в процессе взаимодействия следователя и оперативных сотрудников при расследовании тяжких и особо тяжких преступлений, производство по которым подследственно органам Следственного комитета РФ.

Следственные органы и оперативно-розыскные подразделения обладают специализированными и отличными друг от друга методами и средствами работы, в связи с чем важно, чтобы эти возможности аккумулировались и реализовывались комплексно посредством успешного межведомственного взаимодействия.

Последнее можно определить как согласованную деятельность субъектов, обладающих различными компетенцией, специализацией и уровнем знаний в области уголовного права и процесса, оперативно-розыскной деятельности и криминалистики, основанную на законе и иных нормативно-правовых актах и направленную на достижение такой цели как успешное раскрытие и расследование преступления, а также обеспечение надлежащего применения закона.

Такое взаимодействие предполагает четкое разграничение прав и обязанностей между участниками данной совместной деятельности, каждый из которых действует в рамках своей компетенции с помощью своих средств и методов и в конечном итоге стремится к достижению единой цели — быстрому и полному раскрытию преступления и изобличению виновных.

В следственной практике имеют место множество процессуальных и организационных форм взаимодействия, среди которых обмен информацией, совместное планирование и обсуждение результатов следственных действий и оперативно-розыскных мероприятий, а также производство органом дознания следственных и оперативно-розыскных действий по поручению следователя либо участие оперативного работника в производстве следственных действий.

Наиболее проблемной сферой выступает именно взаимодействие посредством поручений.

Так, в настоящее время в Уголовно-процессуальном кодексе РФ (далее – УПК РФ) не закреплён срок выполнения органом дознания поручений следователя в обычном штатном режиме. Закон содержит лишь указание на необходимость выполнения поручения следователя в срок, не превышающий 10 суток, при направлении поручения в связи с необходимостью производства следственных действий и оперативно-розыскных мероприятий не по месту совершения преступления¹. Таким образом, указанный срок в 10 суток следственной практикой применяется ко всем направляемым следователем поручениям. При этом следует отметить, что в случае необходимости следователь вправе установить иной более короткий срок исполнения поручения.

Однако данные меры на практике не всегда являются эффективными, так как процедура представления следователю результатов исполненного поручения несколько осложнена. В данном случае речь идет не о процедуре предоставления результатов оперативно-розыскной деятельности, сложность которой обусловлена особым статусом представляемой информации, а о процедуре представления результатов исполненного поручения следователя о необходимости производства отдельных следственных и иных процессуальных действий, а также исполнении постановлений о задержании, приводе, аресте.

Так, утвержденная межведомственным приказом правоохранительных органов Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, а также иные ведомственные акты закрепляют возможность представления результатов исполненного органом дознания поручения лишь руководителем органа (подразделения), осуществляющего оперативно-розыскную деятельность. Тогда как целесообразнее бы было дать возможность направлять такие результаты инициатору непосредственно исполнителем поручения, что существенно сократит срок представления ответа на поручение. Как показывает практика объем предъявляемых на подпись руководителю органа (подразделения), осуществляющего оперативно-розыскную дея-

¹ «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 29.07.2017, с изм. от 14.11.2017) (с изм. и доп., вступ. в силу с 01.09.2017) // СПС Консультант плюс.

тельность, документов весьма велик и зачастую эти документы не могут быть подписаны в день их предъявления, в совокупности с выполнением руководителем иных полномочий, предусмотренных его должностной инструкцией, что в некоторых случаях увеличивает общий срок исполнения поручения.

Исходя из вышеизложенного, мы приходим к выводу, что отдельное поручение следователя как процессуальное понятие и действие, являющееся важным и незаменимым аспектом в расследовании уголовного дела, способствующим его скорейшему окончанию и оперативному изобличению виновных, недостаточно регламентировано в действующем уголовно-процессуальном законодательстве, в связи с чем последнее требует внесения изменений в данной части, в том числе путем добавления в УПК РФ статьи «Отдельное поручение следователя», четко регламентирующей его основания, сроки и порядок представления ответа.

Абдурагимова Диана Абдулхаликовна,
курсант Краснодарского университета МВД России;
Сафронов Андрей Алексеевич,
начальник кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

Теоретические основы и актуальные проблемы введения оперативно-розыскного мероприятия «получение компьютерной информации» в оперативно-розыскную деятельность

Безопасность общества и государства является приоритетной задачей, стоящей перед правоохранительными органами и правительством в целом. Для обеспечения безопасности правоохранительным органам приходится постоянно прорабатывать большие объемы информации о деятельности организованных преступных групп, преступных сообществ (организаций). В настоящее время такая информация в основном располагается в различных интернет ресурсах, а также в технических устройствах и средствах связи. В связи с этим появилась проблема собирания компьютерной информации, так как получить доступ к компьютерным данным в интересах оперативно – розыскной деятельности зачастую бывает довольно сложно.

Тема нашего исследования является актуальной в связи с введением 6 июля 2016 г. нового оперативно-розыскного мероприятия (ОРМ) «Получение компьютерной информации», которое утверждено Федеральным законом № 374-ФЗ и вступило в законную силу 20 июля 2016 г.

Появление ОРМ под названием «Получение компьютерной информации» (ПКИ), учитывающего специфику доступа к информации в совре-

менных компьютерных системах, требует детального уяснения сущности, содержания и проработки основ его практического осуществления.

Основной целью является – копирование данных с компьютерных устройств всех типов, которыми пользуются юридические и физические лица.

Его внесение связано с широчайшей распространенностью компьютерной формы представления информации, зачастую оперативно – значимой. Такая информация обладает специфическими свойствами, а также особыми способами ее получения. Все оперативно-розыскные мероприятия направлены на получение информации, независимо от формы ее представления. Тенденция, сложившаяся в последние пять лет, предполагает полный переход от реальной жизни к «интернет-жизни», т.е. подключение к сети почти всех объектов, обслуживающих интересы общества.

Информация – сведения (сообщения, данные), независимо от формы их представления¹.

Компьютерная информация – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.

По мнению доктора наук, профессора А.Л. Осипенко, правильнее было бы говорить даже не об информации, а о данных, которые преобразуются в информацию только при их осмыслении и помещении в определенный контекст.

Злоумышленники, пользуясь компьютерными устройствами могут достаточно быстро обрабатывать данные и пересылать их в любую точку планеты. Особым свойством, активно используемым преступниками при сокрытии следов противоправных деяний, является обезличенный характер компьютерных данных, т.е. отсутствие признаков, прямо указывающих на связь с лицом, их создавшим или подвергшим модификации, а также возможность их быстрого, полного уничтожения. Не менее важно отметить возможность копирования компьютерных данных при полном совпадении исходных данных и копий, которые возможно произвести в неограниченном количестве.

В качестве основных способов несанкционированного доступа к компьютерной информации необходимо выделить следующие:

- преодоление программных средств защиты;
- несанкционированное копирование информации;
- перехват информации в каналах связи;
- внедрение программных закладок и компьютерных вирусов;
- использование аппаратных закладок;

¹ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

- перехват побочных электромагнитных излучений и наводок (ПЭМИН), а также некоторые другие.

ПКИ может производиться в нескольких формах:

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

б) при копировании данных с внешних устройств хранения информации;

в) при получении информации с технических каналов связи и входящих в них промежуточных обслуживающих устройств¹.

Основу ОРМ «Получение компьютерной информации», составляют достаточно сложные в техническом плане и требующие специальной подготовки действия по добыванию хранящейся в компьютерных системах или передаваемой по техническим каналам связи информации о лицах и событиях, вызывающих оперативный интерес. В большинстве случаев их правильное осуществление невозможно без участия специалиста.

По мнению опрошенных, в ходе анкетирования, сотрудников оперативных подразделений мы выяснили, что «получение компьютерной информации» – довольно неизученное оперативно-розыскное мероприятие, которое сотрудники практических подразделений еще не рискуют проводить и смотрят на него с некой опаской. Сотрудники оперативных подразделений Краснодарского края не проводят данное ОРМ и ждут появления точной регламентации организации и тактики его осуществления.

Ранее добывание компьютерной информации осуществлялось в рамках следующих оперативно-розыскных мероприятий:

Снятие информации с технических каналов связи (СИТКС) – ОРМ, заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами работы соответствующих систем и устройств, в том числе излучаемых ими электромагнитных и других полей.

С учетом особенностей данного мероприятия подлежащая съему информация находится в электронно-цифровой форме.

К техническим относятся каналы электросвязи, используемые для передачи и приема знаков, сигналов, письменного текста, изображений, звуков при помощи технических средств по проводной, радио- и другим электромагнитным системам.

Обследование помещений, зданий, сооружений, участков местности и транспортных средств – это ОРМ, заключающееся в непосредственном или опосредованном (с использованием технических средств) визуальном

¹ Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. 2016. №3. URL: <http://cyberleninka.ru/article/n/novoe-operativno-rozysknoe-meropriyatie-poluchenie-kompyuternoy-informatsii-soderzhanie-i-osnovy-osuschestvleniya>

осмотре и изучении (исследовании) указанных объектов с целью выявления лиц, фактов и обстоятельств, имеющих значение для решения задач ОРД.

Получить информацию с электронных носителей возможно было и в рамках проведения данного ОРМ. Но это возможно было сделать, конечно, только в определенном помещении. Дистанционное получение информации возможно осуществить только при проведении нововведенного ОРМ «Получение компьютерной информации».

Сбор образцов для сравнительного исследования – оперативно-розыскное мероприятие, заключающееся в обнаружении, закреплении, изъятии и сохранении предметов и веществ, а также других образцов с целью проверки, оставления лицом следов в определенном месте или на определенных объектах, а также с целью выявления их особенностей и признаков для решения задач оперативно-розыскной деятельности¹.

При проведении указанного ОРМ, как и при «Получении компьютерной информации», возможно копирование и исследование компьютерных программ и файлов.

Анализ выше указанных ОРМ показал, что получение компьютерной информации в том или ином виде представляется возможным и при их проведении.

Те действия, которые предполагает ПКИ оперативные сотрудники осуществляют, в настоящее время, в рамках «Снятие информации с технических каналов связи», «Обследование зданий, сооружений, участков местности и транспортных средств» и «Сбора образцов для сравнительного исследования», чтобы обезопасить себя от ошибок в плане проведения «ПКИ».

По-нашему мнению отличие данного ОРМ от похожих на него заключается в том, что в его рамках можно получить и передать информацию не только при непосредственном контакте с компьютером или другим техническим устройством, а также дистанционно с помощью внедрения в компьютер различных программ, например, шпионского программного обеспечения.

По своей сути «Получение компьютерной информации» охватывает полностью такое ОРМ, как «Снятие информации с технических каналов связи» (СИТКС). Из этих двух ОРМ, понятие «Получение компьютерной информации» является более широким, и включает в себя всю информацию, циркулирующую в каналах связи и находящуюся на средствах вычислительной техники. С практической и теоретической точки зрения в рамках «Получение компьютерной информации» можно осуществлять тот комплекс действий, который реализовывается в «СИТКС», «Сбор образцов

¹ Кушнир И.В. Оперативно-розыскная деятельность, - М 2009.

для сравнительного исследования» и «Обследование зданий, сооружений, участков местности и транспортных средств».

Также нельзя забывать о скором вступлении в силу «Пакета Яровой», 1 июля 2018 года. Появление «ПКИ» возможно связано с принятием данного закона, ведь с помощью введенного ОРМ получать информацию дистанционно станет намного проще. Сам по себе пакет Яровой, согласно законопроекту, операторы связи и «организаторы распространения информации» в интернете должны будут хранить переписку, изображения, звуки, видео и другие сообщения пользователей в течение шести месяцев с момента передачи этих данных. Сам факт о передаче придется хранить на протяжении трех лет. Эта норма вступает в силу с 1 июля 2018 года.

В настоящее время регламентации данного ОРМ не существует в правовой науке Российской Федерации, исходя из этого нельзя говорить о тактике проведения мероприятия и всей его сути. Мы можем лишь предположить в каких целях оно было введено и как его следует проводить оперативным сотрудникам. Но пока не существует даже официальной дефиниции «получения компьютерной информации». А это предполагает, что проведение данного ОРМ пока что невозможно.

Айтманбетов Ислам Муратович,
курсант Новороссийского филиала
Краснодарского университета МВД России;
Кислицын Николай Александрович,
преподаватель кафедры специальных дисциплин
Новороссийский филиал Краснодарского университета МВД

Проблема доверия к сотрудникам подразделений уголовного розыска

Проблема доверия к сотрудникам подразделений уголовного розыска со стороны простых граждан была всегда достаточно актуальна. Сейчас довольно часто всплывает вопрос о доверии к сотрудникам полиции и сотрудникам уголовного розыска в частности. Рассматриваются вопросы о взаимодействии гражданских, общественных организаций с сотрудниками разных подразделений МВД России, но без доверия это кажется невозможным. В интернете, в СМИ часто всплывают новости, видеоролики, статьи о превышении своих полномочий, об избиении жителей и приезжих, коррупции и любой гражданин ставит перед собой вопрос: «Как можно доверять таким людям в погонах?». В любом сериале, телепередаче, фильме «честный опер» живущий на зарплату, является очень нуждающимся человеком, его семья голодает и носит обноски, в то время как те, кто не гнушается «нечестностью», не испытывают больших проблем с финансами и ни в чем себя не отказывают. Я сейчас преувеличиваю, но если такое показывают, значит, в реальной жизни такое встречается не редко.

Если сотрудники подразделений МВД России и в частности сотрудники уголовного розыска не пользуются доверием и уважением среди граждан, это порождает такие проблемы как снижение уровня доверия к самому государству, возникновение ощущения небезопасности, нежелание здравомыслящих граждан поступать на службу в саму полицию и т.д. Именно по этой причине в России нету действующих организаций, оказывающих содействие сотрудникам уголовного розыска. В США и других странах Европы уровень доверия к своим правоохранительным органам находятся на более высоком уровне. В США и в странах западной Европы, действуют общественные организации, как «соседский надзор»¹, «остановим преступность». Как показали исследования зарубежных ученых, многие участники таких программ считают информирование полиции «исполнением своего гражданского долга» и общество полностью поддерживает его, а вот подумайте, что бы сказали про такого гражданина у нас.

По мнению некоторых исследователей именно снижение уровня доверия к российской милиции дало толчок к кардинальным изменениям в системе МВД, а именно издания закона «О полиции», где одним из нововведений как раз стало указание на то, что деятельность полиции должна основываться на принципе общественного доверия и поддержки граждан. Согласно исследованиям, проводимым всероссийским центром изучения общественного мнения, уровень доверия полиции в 2016 году составил 47%, в то время как в 2015 – 46%, а в 2011 – 38%².

Но, даже не смотря на рост доверия, граждане всё так же считают, что сотрудники уголовного розыска не желают заниматься решением их вопросов. Низкий престиж полиции отмечает около 60% населения. Главным источником таких выводов служат СМИ (58,5%), 31,1% граждан судят по опыту обращения к сотрудникам уголовного розыска своих родственников, соседей, друзей, и только 9,4 % – из личного опыта. Чтобы повлиять на население, через СМИ нужно совершать героические поступки, о которых будут вещаться на всю страну, но это невозможно, так как хорошие поступки быстро забываются, под влиянием того, что зрителям не очень интересно слышать про героические поступки, для современного зрителя интересно негативные события с участием сотрудников оперативных подразделений.

Кроме того, для граждан вполне типично судить обо всей структуре по поведению нескольких её представителей, после чего и формируются стереотипы об «оборотнях в погонах». То есть, для того чтобы «завоевать» доверие народа, нужно ломать подобные стереотипы и не давать возможности им появляться. А так как главным источником формирования общественного мнения являются СМИ, то именно за их счёт и нужно формиро-

¹ <https://www.sovremennoepravo.ru/m/articles/view>

² Работа полиции / [Электронный ресурс]: <http://wciom.ru/index.php?id=236&uid=115938>

вать положительный образ сотрудников. Например, после освещения новости о правонарушении со стороны полицейского показать мнения его добропорядочных и законопослушных коллег. Снимать кинокартины с образами героев-полицейских как можно ближе к реальности и самим сюжетом, без сверхъестественного, чтобы ожидания граждан не сталкивались с суровой действительностью. Требуется освещать как можно больше о деятельности полиции, как на службе, так и проведения свободного времени. После выхода телепередачи «Я ПОЛИЦЕЙСКИЙ» был вызван большой интерес к профессии, повысился уровень доверия, ведь в телепередаче показывали, как готовят новых сотрудников полиции на службу. Проект не имеет аналогов на российском телевидении. Почти два месяца курсанты высших учебных заведений МВД России демонстрировали телезрителям беспрецедентного телевизионного шоу «Я – полицейский!» высокий уровень профессиональной подготовки и способности оперативно решать сложнейшие задачи.

В каждой команде было по 5 курсантов от 20 до 22 лет. Они состязались в выполнении крайне сложных, а иногда реально опасных заданий, с которыми могут справиться только профессиональные полицейские. Все задания разработаны с участием экспертов Министерства¹.

Подводя итог вышесказанному, особо подчеркну, когда сотрудники оперативных подразделений работают честно и с полной самоотдачей, делают всё, чтобы обеспечить неотвратимость наказания, относятся к людям доброжелательно и проявляют готовность оказать помощь тем, кто в ней нуждается – в этом случае не нужно делать что-то специально, чтобы доверие населения росло. Это произойдет само собой. Сделать жизнь вокруг лучше и спокойнее можно только при взаимодействии полиции с гражданами. В каждом человеке нужно видеть сторонника. Вместе можно сделать намного больше, чем по отдельности.

Азаров Дмитрий Сергеевич,

курсант Краснодарского университета МВД России;

Стукалов Вячеслав Владимирович,

доцент кафедры оперативно-разыскной деятельности в ОВД

Краснодарского университета МВД России,

кандидат юридических наук

Особенности санкционирования оперативно-розыскного мероприятия «получение компьютерной информации»

Ввиду развития информационных технологий, способы совершения преступлений и обмена информации трансформируются согласно новейшим тенденциям развития общества. Данные изменения происходят в рам-

¹ <https://мвд.рф/tvshow>

ках повсеместной информатизации. Наряду с развитием криминальной среды, усовершенствуется и механизм работы правоохранительных органов по предупреждению и противодействию преступлений.

Доктором юридических наук А.Л. Осипенко и доктором юридических наук В.Ф. Луговик в статье «Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования» было выражено мнение о необходимости совершенствования правового регулирования оперативно-розыскной деятельности в современных условиях, которая определяется и связанными с развитием информационных технологий сложными социальными и технологическими процессами, вызывающими существенное изменение закономерностей образования и концентрации оперативно-значимой информации. Постоянно расширяется спектр технических источников оперативно-розыскных данных, к которым могут быть отнесены различные информационные системы государственных органов и коммерческих структур, в том числе операторов связи, потоки данных от разнообразных датчиков (радиочастотных идентификаторов, GPS-трекеров и т.п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации, сообщения из социальных сетей и иных мест сетевого общения объектов оперативного интереса¹.

В этой же статье, которая была опубликована в 2015 году, ученые провели анализ проекта оперативно-розыскного кодекса Российской Федерации, и пришли к выводу о том, что особую значимость приобретает задача поиска правового закрепления оптимального соотношения между интересами личности и общества.

Одним из шагов на пути совершенствования нормативно-правовой базы в области оперативно-розыскной деятельности было принятие поправок к ФЗ «Об оперативно-розыскной деятельности».

Так Федеральным законом от 06.07.2016 № 374-ФЗ в Федеральный закон «Об оперативно-розыскной деятельности» введено новое оперативно-розыскное мероприятие «Получение компьютерной информации». Целесообразность введения данного оперативно-розыскного мероприятия обусловлена активным использованием сети Интернет криминальными структурами и элементами в целях координации своих согласованных действий и получения информации, необходимой для деятельности вышеуказанных лиц и организаций.

Члены научного сообщества России, высказывали различные мнения о внесении в нормативно-правовую базу, регулирующую оперативно-розыскную деятельность, изменений и целесообразности внесения поясне-

¹Луговик В.Ф., Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. 2015. №2. С. 8.

ний и дополнительной информации в отношении нового вида оперативно-розыскного мероприятия «Получение компьютерной информации».

Именно введение п.15 ст.6 ФЗ «Об ОРД», на данный момент вызывает наибольший интерес, в связи с отсутствием исчерпывающих пояснений в отношении применения данного оперативно-розыскного мероприятия.

Под компьютерной информацией принято понимать информацию, находящуюся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающуюся по каналам связи¹.

Под эту категорию попадает скорее не конкретная информация, а ее форма представления, а именно доступная восприятию ЭВМ. В качестве ЭВМ может выступать техника, начиная с персонального компьютера, сервера, и иного промышленно-вычислительного оборудования, и заканчивая смартфоном распространенного повсеместно, и находящегося практически у каждого человека в пользовании.

Вышеуказанные устройства, так или иначе, аккумулируют и сохраняют информацию о своих пользователях. Это является следствием публикации личной информации гражданами в открытом доступе сети Интернет

В соответствии с ч. 1 ст. 24 Конституции Российской Федерации сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются², учитывая, что граждане публикуют свои сведения в сети Интернет самостоятельно, тем самым дают свое согласие на распространение сведений о себе, при сборе и анализе такой информации права и свободы человека и гражданина не нарушаются.

Таким образом, оперативный сотрудник при осуществлении своих полномочий и при наличии необходимости в сборе информации о лицах, представляющих оперативный интерес, законным образом, как и любой из пользователей сети Интернет, способен путем анализа информации публикуемой в социальной сети, получить сведения об интересующем лице. При этом ни одно из конституционных прав и свобод не будет нарушено.

Методика сбора и анализа «открытой» информации, получаемой в ходе вышеуказанных действий со стороны сотрудников органов, уполномоченных на осуществление оперативно-розыскных мероприятий, требует детального рассмотрения и разработки методических рекомендаций, что осуществить в рамках данной работы ввиду ограниченности объема представляемой информации не представляется возможным.

Следует обратить внимание на иную совокупность способов получения компьютерной информации, которая концептуально отличается от

¹ «Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» (ратифицирован Федеральным законом от 1 октября 2008 г. №164-ФЗ).

² «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к конституции РФ от 21 июля 2014 года № 11-ФКЗ).

упомянутых ранее. Данная совокупность при их реализации потенциально нарушит ряд конституционных прав и свобод человека и гражданина, указанных в статьях 23 и 24 Конституции Российской Федерации, что, с точки зрения законодательства, возможно лишь на основании судебного решения, соответственно, на реализацию данных приемов получения сведений необходимо получить судебное решение.

Одним из способов получения компьютерной информации является негласное получение доступа к устройствам, предназначенным для автоматизированной обработки оцифрованных данных (сетевые и персональные компьютеры, планшеты, смартфоны и др.), лица, представляющего оперативный интерес, путем преодоления защиты доступа специальными техническими устройствами, либо программами. Данный метод возможно реализовать лишь имея специальные технические познания, либо путем привлечения специалистов.

Иной способ получения доступа к данным, находящимся на устройствах, предназначенных для автоматизированной обработки оцифрованных данных, это негласное получение физического доступа к данным устройствам и носителям информации, с последующим их копированием или анализом данных непосредственно с устройства.

Так лицо, представляющее оперативный интерес, вероятно, не даст добровольное согласие на доступ к своим персональным данным. Следовательно нарушение конституционных прав будет неизбежно, и для того чтобы действия сотрудника, уполномоченного на осуществление оперативно-розыскной деятельности, имели законные основания, требуется судебное санкционирование данного оперативно-розыскного мероприятия.

Таким образом, в рамках одного и того же оперативно-розыскного мероприятия получение компьютерной информации оперативный сотрудник может проводить и действия, которые по своей сути не нарушают права и свободы человека и гражданина, и действия нарушающие их. Возникает вопрос, к какой категории оперативно-розыскных мероприятий стоит относить получение компьютерной информации.

Учитывая, что законодательная база непрерывно совершенствуется, по нашему мнению, целесообразно разделить само оперативно-розыскное мероприятие на подкатегории требующее и не требующее санкционирования.

Андреев Сергей Эдуардович,
начальник ОЭБиПК Владимирского ЛО МВД России на транспорте
(адъюнкт кафедры оперативно-разыскной деятельности ОВД
Нижегородской академии МВД России)

Некоторые способы мошенничества в строительной сфере железнодорожного транспорта

Эффективное функционирование железнодорожного транспорта играет исключительную роль в создании условий для модернизации в России, перехода на инновационный путь развития, устойчивого роста национальной экономики.

Важнейшим сектором железнодорожного транспорта является строительная сфера – объект постоянных значительных финансовых вложений.

На железнодорожном транспорте в сферу строительства поступают колоссальные денежные средства. За период с 1999 года в нее инвестировано более 1 трлн. руб. Программой развития железнодорожного транспорта в РФ до 2030 года в указанный сектор планируется направить не менее 12,5 трлн. рублей из средств федерального бюджета и бюджетов субъектов Российской Федерации¹.

Масштабные финансовые потоки в значительной мере определяют тот факт, что строительство является одной из наиболее криминализованных отраслей экономики. Учитывая необходимость строительного процесса, в частности по организации скоростного и высокоскоростного железнодорожного движения, что называется «с нуля», можно не сомневаться, что организованные преступные элементы в сотрудничестве с коррумпированными чиновниками различных рангов попытаются обеспечить себя определённой частью статей бюджетных расходов. Стоит отметить, что направлений для приложения своих преступных действий у подобных дельцов имеется огромное множество.

Всего за 2016 год органами внутренних дел на транспорте согласно статистических данных выявлено 6261 преступление экономической направленности (– 1,8 %), при этом удельный вес регистрируемых экономических преступлений в общей структуре преступности на железнодорожном транспорте, составил 16,8 %, (+ 1,1 % по сравнению с 2015 годом)².

¹ Стратегия развития железнодорожного транспорта в Российской Федерации до 2030 года [Электронный ресурс]: Распоряжение Правительства РФ от 17 июня 2008 г. №877-р. Доступ из справочно-правовой системы «Консультант Плюс».

² Для сравнения необходимо отметить, что в 2016 году удельный вес выявленных экономических преступлений, отнесённых к компетенции ГУЭБ и ПК МВД России, в общей структуре преступности по России был зарегистрирован на уровне 5%.

Экономические преступления, совершаемые на объектах сферы строительства железнодорожного транспорта, обладают существенной спецификой, обусловленной особенностями технологического процесса, документооборота, а также бухгалтерского учёта.

В системе ОАО «РЖД» присутствуют элементы – структурные подразделения, призванные обеспечивать бесперебойное функционирование инфраструктуры железнодорожного транспорта. Среди них:

- дирекции по ремонту пути – призваны организовывать и осуществлять все виды ремонта и реконструкции железнодорожного пути, сооружений и земляного полотна в объёмах, необходимых для безопасного пропуск поездов с установленными скоростями;
- подразделения электрификации и электроснабжения – обеспечения надёжной работы устройств контактной сети, тяговых подстанций, электроснабжения автоблокировки и других стационарных потребителей;
- дистанции централизации, сигнализации и блокировки – ответственны за поддержание в рабочем состоянии систем связи, оповещения на объектах ж/д транспорта.
- и др. (дирекции по эксплуатации зданий и сооружений, дирекции по тепловодоснабжению).

Текущее содержание указанных объектов предполагает, в том числе, проведение ремонтных, строительных работ, которые выполняются сотрудниками соответствующих подразделений ОАО «РЖД» в рамках своих должностных обязанностей.

Мошенничество, ответственность за которое предусмотрена ст. 159 УК Российской Федерации, является одним из распространённых методов реализации вышеуказанных преступных замыслов.

Способ совершения данного преступления – обман или злоупотребление доверием – в объективной стороне мошенничества является конструктивным, совершение хищения иным способом, представляет собой соответственно иной вид хищения (кражу, грабеж, разбой и т.д.). Конкретные приемы, способы обмана или злоупотребления доверием, составляющие криминалистическое понятие способа совершения преступления, входят в криминалистическую характеристику преступления¹.

Остановимся на некоторых способах мошенничества, характерных для сферы строительства железнодорожного транспорта.

1. Фиктивное завышение объёмов предполагаемых к выполнению строительно-монтажных работ.

Является одним из наиболее часто встречающихся способов хищения денежных средств в сфере строительства на объектах инфраструктуры

¹ Голованкова Т.С., Смирнова Н.Н. Способ совершения преступления как элемент криминалистической характеристики мошенничества в сфере строительства // Сборник научных трудов, посвященный 55-летию профессора Э.П. Григониса. Санкт-Петербург. 2017. С.132.

железнодорожного транспорта. В рассматриваемой ситуации строительные организации, выполняющие определённый перечень работ, заведомо включают в их объём и те наименования, которые фактически выполняются (либо уже были выполнены) сотрудниками ОАО «РЖД» в ходе своей повседневной деятельности.

Как показывает практика, в реализации данной схемы по-прежнему используются фирмы – «однодневки», позволяющие осуществлять обналичивание похищаемых денежных средств. Бесспорно, способы совершения данных действий претерпели изменения. И если ранее, в начале двухтысячных, повсеместно встречались факты обналичивания денежных средств путём снятия их по чековым книжкам данных «фирм» при помощи сотрудников банка, нечистых на руку нотариусов, то теперь применяются более сложные и тщательные схемы, подразумевающие использование лицевых счетов физических лиц, электронных кошельков и пр.

2. Фиктивное завышением объёмов и стоимости используемых при выполнении строительно-монтажных работ материалов, вспомогательных технических средств.

Стоит учитывать, что даже незначительное завышение цены на песок, щебень и пр. в предполагаемых к использованию объёмах может составить преступную выгоду со многими нулями. Зачастую и сами материалы и привлекаемая техника могут принадлежать тем или иным подразделениям ОАО «РЖД», принося дополнительный преступный доход при осуществлении мошеннических действий.

В следственной практике имеется немало примеров расследования уголовных дел, возбуждённых по подобным фактам.

Так, следственным отделом Владимирского ЛО МВД России на транспорте было возбуждено и осуществлялось расследование уголовного дела №71038 по ч.4 ст.159 УК РФ по факту хищения денежных средств в сумме более 3 млн. рублей, принадлежащих ОАО «РЖД», руководящими лицами ОАО «Энергомонтажный поезд № 753». Согласно бухгалтерской документации исполнитель на указанную сумму в период 2009-2010 гг. якобы выполнил работы по обустройству обогрева стрелочных переводов на участке «Камешково-Ковров» ГЖД. В то же время в рамках проведения проверочных мероприятий были задокументированы факты того, что фактически данные работы в рассматриваемом временном промежутке были выполнены сотрудниками Ковровской дистанции пути (ПЧ-3) ОАО «РЖД» с привлечением собственных материалов и оборудования.

Практика показывает, что наличие подобных преступных деяний чаще всего невозможно без участия руководящих лиц тех или иных структурных подразделений ОАО «РЖД», призванных контролировать ведение строительного процесса, осуществлять приёмку выполненных работ.

Подтверждением этому может служить уголовное дело № 402190, возбуждённое Нижегородским следственным отделом на транспорте При-

волжского следственного управления на транспорте Следственного комитета России по основаниям, предусмотренным ч. 5 ст.290 УК РФ, в отношении «О», в рассматриваемом периоде занимавшего руководящую должность одного из структурных подразделений ГЖД – филиала ОАО «РЖД».

В период марта 2017 года «О» через посредников получил в виде взятки от представителей коммерческой организации, выполнявшей строительно-монтажные работы на участке «Петушки – Ковров» ГЖД, денежные средства в сумме 800 тысяч рублей за согласование со стороны ОАО «РЖД» актов сдачи-приёмки выполненных работ (форма КС-2) без их фактической проверки.

В настоящее время расследование данного уголовного дела продолжается, осуществляется документирование аналогичных фактов преступной деятельности фигуранта, а также лиц, оказывавших ему содействие в их осуществлении.

3. Мошеннические преступные схемы, связанные с процедурой выкупа земель у собственников на участках, где будут прокладываться новые железнодорожные магистрали.

Реализация стратегии развития железнодорожного транспорта в Российской Федерации до 2030 года предполагает строительство абсолютно новых скоростных и высокоскоростных железнодорожных магистралей. На эти цели планируется направить около 5 трлн. рублей из средств федерального бюджета и бюджетов субъектов Российской Федерации.

Из указанной суммы не менее 1,2 трлн. рублей будет выделено на введение в эксплуатацию до 2023 года высокоскоростной магистрали Москва-Казань. При этом около 40 млрд. руб., выделенных из бюджета и Фонда национального благосостояния (ФНБ), будет потрачено на выкуп земель под строительство магистрали.

Предполагается, что принудительное отчуждение имущества для государственных нужд может быть произведено только при условии предварительного и равноценного возмещения. На возмещение могут претендовать не только их собственники, но и правообладатели. Выкупная цена изымаемого земельного участка определяется по результатам проведенной оценки, при этом возмещению подлежит не только стоимость участка, но и убытки, а также упущенная выгода. В случае, если одновременно с изъятием земельных участков осуществляется изъятие расположенных на них объектов недвижимого имущества, в размер возмещения включается рыночная стоимость этих объектов.

Изложенное является благодатной почвой для применения злоумышленниками мошеннических схем для получения необоснованных выплат. Преступный результат может быть достигнут как путём фиктивного перевода земель из одной категории в другую, так и подделки соответствующих правоустанавливающих документов при коррупционном участии органов местного самоуправления.

Указанные противоправные деяния могут напрямую сказываться на объёмах, а, главное, на качестве выполняемых работ, что впоследствии может создать реальную угрозу безопасности для жизни и здоровья граждан, поскольку железнодорожный транспорт и инфраструктура являются источником повышенной опасности.

Нельзя не упомянуть о том, что в результате данной преступной деятельности бюджет государства недосчитывается огромных денежных средств, которые идут не на развитие и модернизацию транспортного комплекса страны, а попросту разворовываются.

Существует немало примеров совершения подобного рода преступных деяний, наносящих огромный ущерб бюджету страны. Среди них наибольшую огласку получили махинации, выявленные при строительстве космодрома Восточный в Амурской области, при строительстве футбольного стадиона в г. Санкт-Петербурге.

По нашему мнению непременным условием выявления рассматриваемой категории преступлений может являться только всесторонняя и кропотливая деятельность, нацеленная на выявление и документирование всей цепочки организации строительного процесса на железнодорожном транспорте, начиная от осуществления соответствующих конкурсных процедур и заканчивая приёмкой выполненных работ.

Изложенная организация работы предполагает необходимость не только учета специфики особенностей функционирования строительного комплекса железнодорожного транспорта, но и наличие обоснованных методик осуществления организации и тактики реализации основных направлений оперативно-служебной деятельности оперативных подразделений в рассматриваемой сфере.

Ардавов Михаил Мухамединович,
начальник кафедры специальных дисциплин СКИ (ф)
Краснодарского университета МВД России,
кандидат юридических наук, доцент;
Голяндин Николай Петрович,
профессор кафедры специальных дисциплин СКИ (ф)
Краснодарского университета МВД России,
кандидат юридических наук, доцент

О применении нетрадиционных подходов (методов) в оперативно-розыскной деятельности

Последние несколько лет в средствах массовой информации, научной литературе и официальных выступлениях руководства Министерства внутренних дел Российской Федерации стало достаточно часто появляться

словосочетание: «нетрадиционные методы борьбы с преступностью, «нетрадиционные методы оперативно розыскной деятельности (далее по тексту – ОРД)» «методы нетрадиционного получения информации» и т.п.¹

С тем чтобы определиться в предмете статьи необходимо выяснить смысловое значение данного словосочетания.

Используя этимологический подход к понятию «нетрадиционные методы» можно предположить, что в общем смысле это «способы практического осуществления чего-либо», которые не входят в круг «установившихся» или «унаследованных от предшествующего поколения».²

Применительно к ОРД это могут быть мероприятия, действия, способы, приемы (по своей этимологии все указанные понятия являются взаимопределяющими и взаимодополняющими)³, которые ранее не имели широкого распространения в практике оперативно-розыскных органов или вообще не использовались.

При этом необходимо подчеркнуть, что полный перечень оперативно-розыскных мероприятия (далее по тексту – ОРМ) конкретно определен в ст. 6 действующего Федерального закона «Об оперативно-розыскной деятельности» (далее по тексту – ФЗ «Об ОРД») и «...может быть изменен или дополнен только федеральным законом».⁴

Из содержания выше указанной статьи ФЗ «Об ОРД» также следует, что применение органами внутренних дел каких-либо оперативно-розыскных мероприятий не указанных в ней, в том числе нетрадиционных, является открытым нарушением закона.

Поэтому говорить о нетрадиционных методах ОРД можно только в организационно-тактическом аспекте использования законодательно закреплённых оперативно-розыскных мероприятий.

В специальной литературе полемичным также является вопрос о понятии, видах и порядке проведения отдельных ОРМ. Данная проблема возникла в связи с тем, что в ФЗ «Об ОРД» приведен только перечень ОРМ, а их организационно-тактическое наполнение отнесено к компетен-

¹ Марфицин П.Г., Климова О.О. Использование нетрадиционных видов познаний в уголовном судопроизводстве. URL: <http://www.lawtech.ru/pub/netrad.htm/> ; Музеев А.И., Ямалеева А.Н. Некоторые аспекты применения нетрадиционных методов оперативно-розыскной деятельности // Вестник Казанского юридического института МВД России, 2014, № 3, С.112-115.

² Ожегов С.И. Словарь русского языка. - М.: Рус.яз.,1988. С.282, 658.

³ Ожегов С.И. Словарь русского языка. - М.: Рус.яз., 1988. С. 128, 133, 280, 282, 479.

⁴ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016) «Об оперативно-розыскной деятельности». [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=AW&n=201204&fld=134&dst=1000000001,0&rnd=0.6731513152206969#0>, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.11.2017)

ции оперативно-розыскных органов.¹ Указанное обстоятельство приводит к разнотечию сущностного понимания как традиционных ОРМ (опрос, наведение справок, наблюдение, отождествление личности и т.п.) так и тех, которые ранее либо не исследовались в теории ОРД, либо не имели распространения в практике оперативно-розыскных органов (получение компьютерной информации).

На наш взгляд, разрешение указанной проблемы возможно путем внесения в ФЗ «Об ОРД» новеллы, в которой на основании обобщения практики ведомственного регулирования были бы сформулированы общие понятия или определена сущность каждого из перечисленных в ФЗ «Об ОРД» оперативно-розыскных мероприятий.

Исходя из тенденций, наметившихся в криминогенной ситуации в Российской Федерации, количественных и качественных характеристик отдельных групп и видов преступлений, совершаемых как организованными преступными формированиями, так и преступниками одиночками, перед теорией ОРД стоит достаточно сложная задача не отставать от эволюции преступности и своевременно обеспечивать субъекты ОРД научными рекомендациями по повышению эффективности их профессиональной деятельности.²

Разрешение указанной задачи видится в разработке наиболее перспективных в современных условиях направлениях ОРД. Среди них, на наш взгляд, следует выделить:

а) разработка методик получения оперативно- значимой информации, на основе ее программно-аналитической обработки и интегрирования с других информационными потоками;

б) создание организационно-тактических схем по использованию лиц, вовлекаемых в сферу оперативно-розыскной деятельности на основе конфиденциальности, с учетом их национально-религиозных особенностей.

Ограниченные рамки выступления, не дают возможности рассмотреть весь комплекс возникающих при этом проблем. В этой связи мы остановимся на наиболее значимых для Северо-Кавказского региона аспектах осуществления оперативно-розыскной деятельности по получения и последующего использования оперативно-розыскной информации в целях выявления, предупреждения, пресечения и раскрытия фактов противоправной деятельности.

¹ Приказ МВД РФ от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России». [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=216847&fld=134&dst>, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.11.2017)

² Голяндин Н.П., Богданов А.В. Насущные вопросы правового обеспечения оперативно-розыскной деятельности // Вестник экономической безопасности, 2006 № 2. С. 75.

Так, исходя из современных реалий информационного обеспечения оперативно-розыскной деятельности, на наш взгляд, одним из основных поставщиков оперативной информации в борьбе с преступностью становятся подразделения оперативно-розыскной информации (далее по тексту – ПОРИ). Они, обладая сведениями из различных источников и используя аналитические методы обработки информации, могут предоставлять оперативно-значимую информацию, как по запросам оперативных подразделений, так и в инициативном порядке. В практике правоохранительных органов имеются десятки положительных примеров по изобличению участников преступных групп и формирований, в том числе сформированных на этнической основе, с использованием возможностей подразделения оперативно-розыскной информации. Вместе с тем информационно-аналитической работы ПОРИ, в соответствии с ведомственным приказом¹ может реализовываться в рамках осуществления только четыре оперативно-розыскных мероприятий: опроса, наведение справок, сбор образцов для сравнительного исследования, отождествление личности, а также использование конфиденциального содействия граждан. В то же время современные реалии свидетельствуют о геометрической прогрессии увеличении информационных потоков, в первую очередь всемирной информационной системе – Интернет, которую достаточно активно используют криминальные структуры. Поэтому для эффективного функционирования ПОРИ расширение перечня ОРМ, в частности «получение компьютерной информации», становится насущной задачей и предполагает изменения в нормативной регламентации их деятельности.

В теории и практике ОРД в последнее время, как с научной, так и с практической сторон правоохранительной деятельности все больший интерес приобретает использования положений ислама в решении задач борьбы с преступностью.

Данное положение обусловлено целым рядом факторов, среди наиболее значимых из них следует выделить.

Во-первых, ислам для народов России, особенно в местах его массового исповедания (Северный Кавказ, Татарстан, Башкортостан, Крым), всегда выступал как культурно-религиозный феномен, в таком же качестве он возрождается и сейчас.

¹ Приказ МВД РФ от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России». [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: [http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&=216847&fld=134&dst, свободно- Загл. с экрана. - Яз. рус. - \(Дата обращения: 14.11.2017\)](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&=216847&fld=134&dst, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.11.2017))

Во-вторых, учитывая декларируемое Конституцией Российской Федерации «идеологического многообразия» (ст. 13 Конституции России)¹ и расширением круга лиц, поддерживающие мусульманские традиции, ценности религиозных положений ислам приобретает признание не только у населения, но и представителей органов власти.

В – третьих, все чаще в юридической литературе высказывается мнение о правовой системе ислама (шариате), как универсальном средстве в разрешении социальных проблем [8]. Однако такой подход приводит к формированию негативного отношения представителей других религиозных конфессий и иных правовых систем.

В – четвертых, члены экстремистско-террористических организаций и этнических преступных группировок в целях сокрытия криминального образа жизни, придания ему признаков религиозной борьбы с властными структурами или представителя иных религиозных конфессий активно используют отдельных положений ислама.

Кроме того, специалистами безусловно признается региональная специфика преступности, обусловленной местными особенностями. В то же время нормативно-правовая база по вопросам борьбы с преступностью, разрабатываемая в основном с учетом условий центральной части России, не может одинаково эффективно реализовываться во всех субъектах федерации, населенных представителями разных народностей, имеющих свою ментальность. Поэтому, например для Северо-Кавказского региона, одним из способов локализации преступности, может явиться точка зрения правоохранительных органов о необходимости использования положений ислама, как одного из подходов в борьбе с преступностью и создании для него легитимной правовой ниши в рамках специальных институтов права, в частности оперативно-розыскной деятельности.

При этом необходимо подчеркнуть, что современные концепции исламской правовой системы (шариата), ни в коей мере не рассматриваются нами с позиции ее правового признания в социальной жизни светского государства, каковым является Российская Федерация. Нами только ставится вопрос о возможности интегрирования морально-этических воззрений шариата в оперативно-розыскную деятельность.

Под шариатом (с арабского – правильный путь, образ действия) в его общетерминологическом определении понимается совокупность обязательных к исполнению норм и предписаний, установленных Аллахом и переданных им людям через пророка Мухаммада.²

¹ Конституция Российской Федерации. [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: http://www.consultant.ru/document/cons_doc_LAW_28399/, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.11.2017)

² Ислам: Энциклопедический словарь / отв. ред. С. М. Прозоров. - М.: Наука, ГРВЛ, 1991. С. 292.

Мусульмане относятся к шариату, как божественному откровению, поэтому считают его священным и вечным. При таком подходе шариат – религиозная совесть мусульманина, основанная на вере и нравственности. Ее проявление осуществляется в исполнении религиозных обязанностей и строгом соблюдении установленных дозволений и запретов, которые не могут быть нарушены ни человеком в процессе своей жизнедеятельности, ни государственными властями при принятии законов и их исполнении. Любое правонарушение в исламском праве рассматривается как неподчинение воле Всевышнего, за которое следует наказание.

В нормативно-правовой части шариата (фикх) человеческие поступки с точки зрения их запрета и позвольности разделены на пять степеней (ахам аль-хамса): запретные (харам, мазхур), порицаемые (макрух); обязательные (фард, ваджиб); рекомендуемые и одобряемые (суннат, мандуб, мустахабб); общедозволенные и нейтральные (мубах, джаиз).¹

Игнорирование или незнание этих канонических предписаний приводят к тому, что в тех случаях, когда мусульманин при осуществлении ОРД будет склоняться оперативным работником к совершению действий, относящихся к запретным или порицаемым, то вряд ли при этом будут достигнуты положительные результаты.

Поэтому познание оперативным составом органов внутренних дел основных положений ислама в целом и шариата в частности, правильное их использование в своей профессиональной деятельности становится объективной необходимостью.

Однако данное обстоятельство недооценивается в системе правоохранительных органов. В ходе проведенного нами опроса более 300 сотрудников оперативных аппаратов, дислоцирующихся на территории Северного Кавказа, только 18% считают, что знают основные положения шариата, 31% считают, что они знакомы с отдельными положениями шариата и почти каждый второй (43%) оценивает свои знания шариата как недостаточными для успешного использования в своей практической деятельности. В то же время достаточно спорное толкование дискуссионных догматов положений ислама и мусульманского права активно используются экстремистско-террористическими организациями в вербовке новых членов[2].²

Достижение истинных целей шариата, освоение обществом его основополагающих ценностей могут быть обеспечены только путями и способами, которые отражают природу самого шариата, в частности, такие его начала, как усредненность, умеренность, постепенность, избегание край-

¹ Ислам: Энциклопедический словарь / отв. ред. С. М. Прозоров. - М.: Наука, ГРВЛ, 1991. С. 292.

² Голядин Н.П., Горячев А.В. Мотивации вербовки в экстремистские и террористические организации. // Вестник Краснодарского университета МВД России, 2013, № 2. С 38.

ностей, не нанесение вреда, не обременение человека. А это требует глубоких знаний самого шариата.

В то же время в высших учебных заведениях МВД России фактически отсутствует система подготовки специалистов по данной проблеме. Поэтому целесообразна и своевременна постановка вопроса о введении в систему профессиональной подготовки сотрудников для правоохранительных органов специальных курсов, предусматривающих изучение основных положений ислама. Цель таких курсов очевидна – последующее использование полученных знаний в организации борьбы с преступностью и обеспечения охраны общественного порядка в регионах Северного Кавказа.

Литература:

Белый Андрей Григорьевич,
заместитель начальника кафедры ОРД в ОВД
Краснодарского университета МВД России
кандидат юридических наук, доцент;

Киселев Сергей Сергеевич,
старший преподаватель кафедры уголовного права и криминологии
Краснодарского университета МВД России,
кандидат юридических наук

Состояние оперативной обстановки в сфере противодействия экстремизму и терроризму в Северо-Кавказском федеральном округе

События последних лет в России и мире свидетельствуют о возрастании и расширении террористической агрессии: страшная трагедия 2004 г. в Беслане; террористические акты 2010 г. в Москве, Ставрополе, Владикавказе, Кизляре; взрыв в московском аэропорту «Домодедово» в январе 2011 г.; убийства и покушения на жизнь духовенства, представителей зарегистрированных религиозных течений в Республиках Дагестан, Ингушетия, Кабардино-Балкария в августе – сентябре 2012 г.; взрывы в Волгограде (декабрь 2013 г.); нападение боевиков Кавказского Эмирата на Грозный в декабре 2014 г.; многочисленные террористические акты в странах Европы в течение 2015-2017 гг.; нападение на здание ОВД в селе Новоселицкое Ставропольского края в апреле 2016 г.; нападение на базу Росгвардии в Чеченской Республике (март 2017 г.); взрыв в метро Санкт-Петербурга в апреле 2017 г., практически ежемесячные посягательства на сотрудников полиции и их семьи на Северном Кавказе и других регионах России.

При этом вызывает опасение возрастание степени адаптивности экстремизма и терроризма к правовым и социальным барьерам, что отражается в усложнении форм агрессии, ежегодном росте преступлений данной направленности, специальном обучении боевиков на Ближнем Востоке.

Проблемными остаются вопросы, связанные с выявлением причин и условий экстремистских проявлений и проработанностью организационных механизмов, регулирующих противодействие экстремизму и терроризму, соответствующими органами государственной власти России.

Особенно остро эта проблема стоит в Северо-Кавказском федеральном округе, в рамках субъектов которого встречаются практически все виды конфликтов. А зародившиеся здесь достаточно давно проблемы в области межэтнических и межконфессиональных отношений влекут постоянный рост недоверия к власти, ненависти и вражды к социальным группам, мешают установлению стабильности в округе и в целом в России, влекут человеческие жертвы.

Именно поэтому необходима соответствующая научная база, позволяющая субъектам противодействия экстремизму и терроризму качественно решать возложенные на них задачи, рефлексировать и действовать на опережение в сложных условиях межнациональных отношений на Северном Кавказе.

Согласно имеющимся данным оперативная обстановка в Северо-Кавказском федеральном округе в течение 2013-2016 гг. серьезно осложняется, но остается под контролем органов внутренних дел.

Особое опасение вызывает тот факт, что по данным ГИАЦ МВД России на территории данных субъектов за последние 4 года стабильно фиксируется серьезный прирост преступлений террористического характера. Так, например, в 2013 г. на территории СК ФО было зарегистрировано 579¹ таких фактов, а за 12 месяцев 2016 года уже 1572 подобных общественно опасных деяний, что на 34,6% больше АППГ и составляет 70,1% от всех преступлений данной категории, совершенных в Российской Федерации (2227).

По данным Центра по противодействию экстремизму ГУ МВД России по СК ФО, рост показателей террористической активности в Северо-Кавказском федеральном округе объясняется активизацией деятельности органов охраны правопорядка, поскольку подавляющее большинство учтенных в статистике террористических преступлений поставлены на учет по уголовным делам, возбужденным по инициативно выявленным сотрудниками правоохранительных органов фактам выезда граждан Российской Федерации для участия в вооруженных конфликтах в Сирии и Ираке, а также преступными деяниями террористического характера, совершенными в сети Интернет.

В отличие от террористических преступлений, уровень, динамика и структура преступлений экстремистской направленности в СК ФО практически не изменилась. При этом сопоставление количества экстремистских преступлений,

¹ Обзор состояния оперативной обстановки в Северо-Кавказском федеральном округе и о принятых мерах в сфере противодействия экстремизму и терроризму за 12 месяцев 2013 года. - Нальчик, 2014. - С. 2.

зарегистрированных в СК ФО, в сравнении с общим их числом совершенных по Российской Федерации выявляет оптимистичную тенденцию, в рамках которой показатели динамики по округам отстают от общероссийских (пусть и незначительно). Это дает основания для вывода о постепенной стабилизации обстановки на Северном Кавказе в данной сфере.

Следует учитывать, что относительная стабилизация динамики зарегистрированных преступлений экстремистской направленности в среднем по округам еще не является достаточным основанием для вывода о стабилизации оперативной обстановки в СК ФО в целом, поскольку степень радикализации общества на Северном Кавказе по-прежнему остается на достаточно высоком уровне, о чем свидетельствуют данные о лицах, выезжающих в Сирию и Ирак для диверсионной подготовки и участия в боевых действиях на стороне международных террористических организаций (далее – МТО), а также возвратившихся с преступными целями на территорию России после такой боевой практики.

Ключевую роль в этих процессах безусловно играют действующие на территории СК ФО диверсионно-террористические группы.

Примечательно, что за последние годы на территории анализируемых округов сократилась как численность этих групп, так и численность установленных участников НВФ. При этом активность религиозно-экстремистского бандподполья, целью которого является создание так называемого «халифата», по-прежнему выступает одним из основных факторов, дестабилизирующим оперативную обстановку в СК ФО.

И невзирая на понесенные значительные потери, бандподполье по-прежнему сохраняет свой потенциал. В 2017 г. наибольшие опасения вызывают Республика Дагестан – 10 ДТГ (более 20 участников).

Данные группы составляют основную часть бандподполья и входят в состав МТО «Исламское Государство», что подтверждается имеющей место в сети Интернет публичной «присягой на верность» лидеру ИГ, которую дали руководители 6 из 10 бандгрупп (Кадарская, Губденская, Махачкалинская, Хасавюртовская, Кизилюртовская, Цумадинская). В подчинении т.н. «Имарата Кавказ» остались 4 бандгруппы (Харачинская, Балаханнинская, Шамильская, Хунзахская)².

Лидером террористического бандподполья на территории РД являлся Асельдеров Рустам Магомедович, 1981 г.р., т.н. «Амир Вилайята Дагестан» по версии МТО «ИГ», находившийся в федеральном розыске (ликвидирован в результате спецоперации 03.12.2016 г.). Новый лидер не назначен. Тем не менее, по сведениям Центра по противодействию экстремизму МВД Республики Дагестан, за 2016 г. на территории субъекта порядка 40 лиц были вовлечены в деятельность бандподполья: из них от 16 до 20 лет – 9, от 20 до 25 лет – 13, от 25 до 30 лет – 10, от 30 до 35 лет – 4, от 35 до 40 лет – 4. Часть из них уничтожена к началу 2017 г.

Не менее опасными представляются 3 группы, действующие на территории Чеченской Республики (Веденское направление, Урус-Мартановское и Ачхой-Мартановское направление, Ножай-Юртовское, Гудермеское и Курчалоевское направление) численностью более 25 боевиков. Возглавляет бандподполье т.н. «Амир Вилаята Нохчийчоь» Бютукаев А.А., «Хамзат», 1974 г.р., в настоящее время находится в федеральном розыске по ч. 2 ст. 208 УК РФ (организационно не включен в состав бандгрупп).

В Республике Ингушетия бандподполье «Вилайат Галгайче», как и в Чеченской Республике делится структурно на три сектора, именуемых по названиям районов республики. На январь 2017 г. в указанных секторах действуют 3 ДТГ установленной численностью более 35 человек, структурно входящих в МТО «Исламское Государство»: 1) Сунженская (14 участников); 2) Малгобекская (11 участников); 3) Назрановская (12 участников).

В остальных субъектах СК ФО согласно данным Центра по противодействию экстремизму ГУ МВД России по СК ФО, деятельности террористических и экстремистских групп и организаций не выявлено. Однако это не означает, что там нет «спящих» ячеек боевиков и сочувствующих им готовых не только оказать пособническую помощь, но и при других условиях (идеологической обработке, родственной поддержке, «мусульманской» солидарности) участвовать в террористических и экстремистских акциях.

В связи с этим требует пристального внимания религиозный фанатизм, который используется лидерами бандподполья для подготовки молодежи к совершению диверсионно-террористических актов. В том числе новообращенных мусульман – т.н. «неофитов» в качестве террористов-смертников.

По данным, предоставленным Центрами по противодействию экстремизму, сегодня имеется информация в отношении 1120 лиц, сменивших вероисповедание на ислам (КБР-30, КЧР-119, РД-218, РИ-159, РСО-20, СК-445, ЧР-129), часть которых принимает его радикально-салафитскую форму.

Новообращенные особо ценны для лидеров экстремистов. Они не выглядят подозрительно для правоохранительных органов, но при этом особенно агрессивны вследствие применяющихся к ним методов психологической обработки со стороны вербовщиков. В Республике Дагестан сторонники салафизма объединены в политизированную организацию «Ахлю Сунна валь Джамаа», которая нуждается в постоянном оперативном контроле со стороны правоохранительных органов.

Кроме того, в настоящее время на территории СК ФО действует целый ряд нетрадиционных для России конфессий. Наиболее распространены христианские сектантские организации, такие как: «Свидетели Иеговы» (деятельность запрещена Верховным Судом Российской Федерации 20 ап-

реля 2017 г.), пятидесятнические группы, «Церковь Адвентистов Седьмого дня». Имеются подразделения неоиндуистской секты «Общество сознания Кришны» и другие тоталитарные течения нетрадиционных религиозных верований.

Наиболее распространенной в СК ФО является религиозная секта «Свидетели Иеговы» – согласно данным, полученным из ЦПЭ МВД, ГУ МВД России по СК ФО, ее деятельность не имеет места в Чеченской Республике, в Ингушетии и Дагестане. На территории остальных субъектов округа ее общины присутствуют повсеместно.

Общая оценочная численность адептов организации «Свидетели Иеговы» на территории СК ФО составляет порядка 35-40 тыс. человек. Примечательно, что решение Верховного Суда Российской Федерации в отношении Религиозной организации «Управленческий центр Свидетелей Иеговых в России» о запрете деятельности от 20 апреля 2017 г. распространяется не на всех. Так как организация официально единой структуры не имеет, поскольку во избежание запрета деятельности всех общин организации одновременно, каждая из них регистрируется в территориальных органах юстиции самостоятельно. Представляется, что в текущем году, силы правоохранительных органов будут направлены на полную ликвидацию деятельности данной организации.

В округе наибольшую активность эта секта проявляет на территории Ставропольского края, где действуют 42 общины «Свидетелей Иеговы». Согласно данным ЦПЭ ГУ МВД России по Ставропольскому краю, примерная численность адептов составляет 20-25 тыс. человек.

Имеют место также общины неоязыческого толка:

1) региональное общественное движение «Центр развития русской этнической культуры «РАРОГЪ»», возникшее вследствие объединения в 2011 году неоязыческих организаций деструктивного толка в регионе КМВ жителем г. Лермонтов Ворошевым Р.Р.

Члены «Рарога» имеют связи с украинскими неоязыческими и праворадикальными националистическими структурами. Также были установлены и зафиксированы факты участия адептов входящей в «Рарогъ» общины «Скифия» (г. Пятигорск) в вооруженном конфликте на стороне добровольческого батальона «Айдар» национальной гвардии Украины.

Лица, входящие в данную организацию, вопреки уставным целям, активно участвуют в политических процессах, митингах, демонстрациях, неоднократно организовывали резонансные протестные акции, в ходе которых осуществлялось давление на представителей органов власти и правоохранительных органов, в том числе по расследованию «громких» преступлений в целях придания им «политической окраски».

2) Ставропольская община Союза Славянских Общин Славянской Родной Веры – Родноверы. Лидер – Акинтьев А.В. («Озар»). Бывший лидер –

Букреев С.В. («Яромир») вступил в батальон «Азов», в настоящее время объявлен в розыск.

Также отмечена активность иных псевдохристианских организаций:

1) «Церковь Иисуса Христа последних дней» (мормоны). Численность членов секты составляет около 30 человек. По имеющейся информации, финансирование деструктивной деятельности секты осуществляется из США¹, проповедниками секты являются 2 гражданина указанного государства. Периодически производится «ротация» проповедников.

2) «Древнерусская инглистическая церковь православных староверов инглингов». Согласно заключению религиоведческого исследования, в деятельности данного религиозного объединения содержатся проявления экстремистской направленности (элементы теории расового превосходства, национализма, в том числе материалы антисемитского содержания, направленные против конституционных основ государства, запрещенная символика, свастика). Ставропольским краевым судом 21.08.2015 г. указанная организация признана экстремистской и ее деятельность запрещена.

3) Церковь «Новое поколение». Лидер – Савин Дмитрий Валерьевич. 26.11.1983 г.р. Относится к разряду харизматических неопятидесятнических религиозных вероучений. Адептам внушают, что для богатства и счастья необходимо приносить деньги в секту. Среди сподвижников принято считать, что больной ребенок проклят Богом и заслуживает смерти.

В целом нельзя недооценивать деструктивный характер всех экстремистских организаций, действующих на территории СК ФО, даже в том случае если их деятельность напрямую не связана с агрессивными действиями и насилием. Особенно когда речь идет о молодежных организациях.

В настоящее время, по данным МВД, ГУ МВД субъектов РФ в СК ФО на территории округа неформальные молодежные организации деструктивного характера в большей степени существуют на территории Ставропольского края.

На оперативном контроле находятся 230 лиц, из них: фанаты футбольной команды «Динамо» (Ставрополь) – 42, представители Ставропольского молодежного движения «Русская пробежка» – 6, фанаты футбольного клуба «Локомотив КМВ» (г. Минеральные – Воды) – 8, реестровое казачество – 15, не реестровое казачество – 14, «Союз славянских общин славянской родной веры (ССОСРВ) (родноверы) – 12, родноверы «Рарог» – 16, инглинги – 17, незарегистрированные организации – 22, КПКР – 4, активные блогеры – 23, секты и иные религиозные организации – 30, «Вече Руси» – 3, «Ополченцы» – 18 человек.

¹ Обзор состояния оперативной обстановки в Северо-Кавказском федеральном округе и о принятых мерах в сфере противодействия экстремизму и терроризму за 12 месяцев 2016 года. - Нальчик, 2017. - С. 20.

Как отмечалось выше, сегодня одной из главных особенностей оперативной обстановки в сфере противодействия экстремизму и терроризму в Северо-Кавказском федеральном округе является проблема зарубежной диверсионной подготовки боевиков НВФ и возвращение их на территорию России.

При этом следует учитывать, что в результате успешных спецопераций правоохранительных органов, в составе бандгрупп, действующих на территории СК ФО, почти не осталось опытных боевиков, имеющих достаточный боевой опыт и способных оказать должное сопротивление при огневых контактах.

В такой ситуации простое восполнение численного состава бандформирований новобранцами не позволяет изменить положение дел и вернуть влияние, которым незаконные вооруженные формирования обладали еще 3-4 года назад, поскольку вступающая в бандгруппы молодежь не подготовлена и не обучена. В связи с этим бандлидеры направляют своих сторонников на «стажировку» в Сирию и Ирак, где в условиях реальных боевых действий они получают необходимый опыт и проходят идеологическую обработку.

По данным МВД, ГУ МВД субъектов РФ в СК ФО, для участия в боевых действиях на стороне международных террористических организаций в Сирии и Ираке убыли 2677 жителей округа, из которых 446 уничтожено, 2040 объявлено в федеральный розыск, 806 – в международный, в оперативный – 319. Возбуждено 1506 уголовных дел.

В этом контексте особую роль играют лица, осуществляющие вербовочную деятельность.

Существенные потери, которые на протяжении последних лет несет экстремистское подполье, обусловили рост активности идеологов террористических организаций, направленной на восстановление его численности за счет новых сторонников.

В 2013-2016 годах органами внутренних дел установлены 17 лиц (КЧР- 1, РД-6, РСО-1, СК-1, ЧР-8), осуществлявших вербовочную деятельность по вовлечению в ряды НВФ, в том числе и находясь за рубежом.

В целях вовлечения в противоправную деятельность новых участников и расширения пособнической базы, лидеры и идеологи МТО наращивают пропаганду экстремистской идеологии в молодежной среде, в т.ч. с использованием современных информационных технологий. На экстремистских интернет-сайтах регулярно размещаются аудио-видеоматериалы, содержащие комментарии с оправданием идеологии терроризма и направленных на разжигание межэтнической и межконфессиональной вражды.

За 12 месяцев 2016 года Центрами по противодействию экстремизму органов внутренних дел, дислоцированных на территории субъектов СК ФО, в процессе мониторинга сети Интернет был выявлен 1081 источник

информации, содержащий материалы с признаками идеологии экстремизма: КБР-8, КЧР-12, РД-466, РИ-4, РСО-51, СК-55, ЧР-39, ГУ-446.

В целом прогнозируется значительная активация использования членами экстремистских и террористических группировок средств сети «Интернет», опыт ряда стран показывает нам, что минимальные затраты на социальные сети могут мобилизовывать массы людей и приводить к революционным ситуациям.

Относительно террористических угроз следует учитывать новые формы атак в местах массового скопления людей, использованных во Франции, Германии, Израиле, США.

В целях недопущения указанных выше угроз необходимо комплексное решение обеспечения безопасности на территории СК ФО, в связи с чем, требуется анализ причин и условий рассматриваемых общественно опасных явлений, разработка комплекса соответствующих мер.

Бильданова Лейсан Ильгизовна,
курсант Казанского юридического института МВД России

Оперативная провокация как способ фальсификации (ч. 4 ст. 303 УК РФ)

Важнейшим направлением любого государства является осуществление правоохранительной функции. Успешная и эффективная реализация уголовного закона, предупреждение преступлений, неизбежность наказания за их совершение обеспечиваются посредством уголовного судопроизводства и оперативно-розыскной деятельности.

Учитывая усмирительный потенциал отношений, развивающихся в сфере уголовного судопроизводства, необходимо, чтобы все принимаемые решения были обоснованными и законными, что исключает из практики правоохранительных органов провокационно-подстрекательские действия.

Приведем пример превышения должностных полномочий, повлекших тяжкие последствия (ч.3 ст. 286 УК РФ), сотрудниками ГУЭБиПК, которые организовали оперативное мероприятие с участием на конфиденциальной основе лица, обратившееся к гражданам, имевшим намерение совершить мошеннические действия, для изобличения последних. Потерпевшие планировали от провокации получить от конфиденента 1,2 млн долларов якобы за место в высшем совете партии «Единая Россия». Безусловно, возможности выполнить свои обещания они не имели, а денежные средства собирались похитить¹. Таким образом, если будет установлено, что конфиденент по поручению оперативных сотрудников инициативно об-

¹ У полицейского не хватило полномочий на мошенника // Коммерсантъ. 2016. 17 декабря.

ратился к потенциальным мошенникам, то имела место оперативная провокация.

Согласно части 8 ст. 5 Федерального закона от 12 августа 1995 года №144-ФЗ «Об оперативно-розыскной деятельности» законодатель прямо запрещает органам (должностным лицам), осуществляющим оперативно-розыскную деятельность, подстрекать, склонять, побуждать граждан в прямой или косвенной форме к совершению противоправных действий, иными словами, провоцировать граждан к совершению преступления¹.

Отметим, что проведение оперативного эксперимента возможно после осуществления лицом действий, свидетельствующих о его приготовлении к конкретному преступлению. Мероприятие будет правомерным, если умысел на совершение преступления сформировался у разрабатываемого без влияния оперативных сотрудников и конфиденентов.

Сотрудники правоохранительных органов, совершая провокационно-подстрекательские действия, могут иметь желание пресечь преступную деятельность лица, в отношении которого поступила информация о ранее совершенных им преступных деяниях. Но создание «благоприятной» обстановки для совершения преступления будет признано незаконным, если с требованием о передаче взятки, с предложением о сбыте наркотиков выступило само спровоцированное лицо. В соответствии с положениями ФЗ «Об оперативно-розыскной деятельности» проведение оперативно-розыскных мероприятий допускается для выявления уже готовящихся, а не лишь возможных в принципе преступлений. Также, согласно п.34 Постановления Пленума Верховного Суда РФ от 9 июля 2013 года № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» разъясняется, что провокационно-подстрекательские действия состоят в передаче взятки по предложению или с согласия должностного лица, когда такое предложение или согласие было получено путем склонения к получению определенных ценностей при обстоятельствах, свидетельствующих о том, что без вмешательства сотрудников правоохранительных органов умысел на их получение не возник бы и преступление не было бы совершено.

По сложившейся практике совершение сотрудниками оперативных подразделений провокационно-подстрекательских действий квалифицируется как превышение должностных полномочий (ст. 286 УК РФ), тем самым следователи игнорируют ч.4 ст. 303 УК РФ, которая предусматривает ответственность за фальсификацию результатов оперативно-розыскной деятельности в целях уголовного преследования лица, заведомо непричастного к совершению преступления.

Многие авторы в качестве ключевого признака превышения должностных полномочий выделяют его «явность». Так, Б.Волженкин поясняет

¹ Определение Конституционного Суда РФ от 22 апреля 2014 г. № 845-О.

данный признак следующим образом: «должностное лицо осознает, что совершает действие, которое явно, очевидно для него самого выходит за пределы имеющихся у него полномочий»¹. А.Светлов упор делает на «субъективный момент, то есть виновный знает объемы своих служебных и властных компетенций, явно превышает ее»². Бесспорно, подход известных ученых не сужает сферы уголовной противоправности при оценке общественно опасного поведения лиц.

Применительно к ч. 2 ст. 303 УК РФ, фальсификация (подделка) – сознательное искажение представляемых доказательств. Таким образом, искаженными следует признавать результаты оперативно-розыскного мероприятия, полученные путем подстрекательства, склонения, побуждения в прямой или косвенной форме разрабатываемых лиц к совершению правонарушений.

Б. Волженкин пишет, что ответственность за превышение должностных полномочий, предусмотренных ст. 286 УК РФ, наступает в том случае, когда должностное лицо обладало какими-либо полномочиями по отношению к потерпевшему лицу (или организации), права и интересы которых существенно нарушены действиями должностного лица. То есть субъект воздействует на потерпевшего. В некоторых случаях можно квалифицировать принуждение оперативным работником гражданина к негласному сотрудничеству, участию в оперативно-розыскных мероприятиях. Однако отметим, что потерпевшими являются все-таки не лица, привлекаемые к конфиденциальному сотрудничеству, а разрабатываемые лица.

Действия первого вице-губернатора Амурской области К., были квалифицированы как превышение должностных полномочий. По данным следствия, он требовал от фирм и предпринимателей перечислять 1% от оборота на счет жилищного фонда при губернаторе Амурской области за предоставление квот на привлечение иностранных работников. Ущерб, причиненный им, составил около полутора миллионов рублей³. Требования были, очевидно, противоправными.

Иное дело, когда провокационно-подстрекательские действия, представляющие собой законспирированную негласную организационную деятельность сотрудников правоохранительных органов, направленное на возбуждение у разрабатываемого лица желания совершить преступление. Как правило, в непосредственный контакт с разрабатываемым вступает не оперативный сотрудник, а лицо, оказывающее содействие на конфиденциальной основе.

Преступление, предусмотренное ст. 286 УК РФ, предполагает выход субъекта за пределы одного из трех видов полномочий, указанных в п. 1 примечания к ст. 285 УК РФ. Утверждение, согласно которому соверше-

¹ Волженкин Б.В. Служебные преступления. М., 2000. С. 157.

² Светлов А.Я. Ответственность за должностные преступления. Киев, 1978. С. 173.

³ Российская газета. 2009. 20 февраля.

ние провокационно-подстрекательских действий является выходом за пределы властных полномочий, спорно. Оперативно-розыскная деятельность не предполагает государственного принуждения, при ее осуществлении не возникают отношения власти и подчинения. В оперативно-розыскной деятельности государственное регулирование заключается в установлении системы гарантий законности, соблюдения прав граждан при проведении оперативно-розыскных мероприятий. При их осуществлении оперативные сотрудники не наделены распорядительными полномочиями в отношении лиц, не находящихся от них в служебной зависимости, а также правом принимать решения, обязательное для исполнения гражданами и организациями. Итак, если властных полномочий в сфере оперативно-розыскной деятельности у сотрудников правоохранительных органов нет, то они не могут быть и превышены. Провокационно-подстрекательские действия все-таки следует квалифицировать по ч. 4 ст. 303 УК РФ.

Известно, что при проведении оперативно-розыскных мероприятий материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, а также материальные объекты, в соответствии с уголовно-процессуальным законодательством могут быть признаны вещественными доказательствами. Но перечисленные предметы и материалы могут быть получены непосредственно конфидентом, возможно, и незаконно. Однако субъектом преступления, предусмотренного ч. 4 ст. 303 УК РФ, признано лицо, уполномоченное на проведение оперативно-розыскного мероприятия, то есть сотрудник органа, осуществляющего оперативно-розыскную деятельность.

Нередко в судебной практике возникают проблемы с признанием субъектом фальсификации оперативно-розыскной деятельности не только обычных граждан, но и сотрудников оперативных подразделений.

Субъектами преступлений, предусмотренных ч. 4 ст. 303 УК РФ, необходимо признать не только оперативных работников, но и иных лиц, если они действуют с ведома лица, уполномоченного на проведение оперативно-розыскного мероприятия, с целью последующего использования фальсифицированных результатов оперативно-розыскной деятельности. Считаем, изменение нормы позволит снять вопрос о юридической оценке действий того, кто фактически принял участие в фальсификации, осуществляемой сотрудниками правоохранительных органов. Приняв во внимание изложенное, предлагаем следующую редакцию ч. 4 ст. 303 УК РФ:

«4. Фальсификация результатов оперативно-розыскной деятельности лицом, уполномоченным на проведение оперативно-розыскных мероприятий, а равно другим лицом с ведома лица, уполномоченного на проведение оперативно-розыскных мероприятий, в целях уголовного преследования лица, заведомо непричастного к совершению преступления, либо в целях причинения вреда чести, достоинству и деловой репутации- ...».

Итак, организация сотрудниками органов, осуществляющих оперативно-розыскную деятельность, провокационно-подстрекательских действий и представление результатов, полученных в ходе мероприятия, содержит признаки преступления, предусмотренного ч. 4 ст. 303 УК РФ. Признаки преступления, предусмотренные статьей 286 УК РФ, не присущи для оперативной провокации.

Габисов Сергей Валерьевич,
курсант Краснодарского университета МВД России;
Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Выявление фактов мошенничества, связанных с использованием бесконтактной оплаты

Актуальность проблемы мошенничества, связанного с использованием бесконтактной оплаты обусловлена тем, что наряду с применением новых технологий в сфере банковских услуг растут и факты мошенничества в данной сфере, в связи с чем проблема требует особого внимания, поскольку риски этой сферы значительно подрывают доверие к банковской деятельности и несут опасность дестабилизации всей финансовой системы. Выявлением фактов мошенничества данной сферы осуществляет Управление «К» МВД России.

В связи с тем, что предметом настоящего исследования является хищения, совершенные с использованием только расчетных и кредитных карт (как разновидностей банковских карт), то мы не будем останавливаться на более подробной классификации платежных карт.

Что такое бесконтактная оплата? Существуют следующие виды бесконтактной оплаты:

1. Карты с технологией бесконтактной оплаты – это карты, которые оснащены встроенными чипом и антенной, передающими по радиоканалу на бесконтактный терминал информацию о платеже.

2. Мобильные приложения для телефонов (Apple Pay, Android Pay и Samsung Pay). Порядок действий схож с карточкой, но для оплаты сама карточка вам не нужна. Данные приложения предусмотрены для телефонов, с поддержкой технологии NFC, которые позволяют расплатиться в магазине точно также, как банковской картой.

Достоинства бесконтактной оплаты:

- простота оплаты (не нужно вводить ПИН-код при совершении платежа, установлен лимит в 1000 рублей для одноразового платежа).
- высокую скорость проведения транзакции;
- нет необходимости передавать свою банковскую карту постороннему лицу (кассиру);
- срок службы карты по сравнению с обычными повышен.

Недостатки бесконтактной оплаты:

Помимо основных, общеизвестных существует еще один, это безопасность (несмотря на то, что платежные системы утверждают, что бесконтактные платежи надежно защищены, на деле мошенники находят способы считывать данные с таких карт без ведома их владельцев). Известны случаи использования самодельных RFID-ридеров. Единственный вариант защиты от подобного рода хищений – различные чехлы (кошельки), экранирующие радиосигнал.¹

Сама банковская платежная карта не является предметом преступного посягательства, поскольку она представляет собой лишь инструмент доступа к денежным средствам владельца карты, размещенным на его счете, которые являются предметом преступного посягательства.

Преступления данного вида не раскрываются по «горячим следам», а классические методы проведения оперативно-розыскных мероприятий не дают должного эффекта, лишь позволяют подтвердить факт хищения, а не выявить конкретных лиц, их совершающих. Во многих случаях установление злоумышленников невозможно. Что касается сбора доказательной базы, то и тут возникают сложности. Основная проблема заключается в том, что для установления данных счета мошенника необходимо получить разрешение суда, что существенно усложняет процесс изобличения мошенника. Так же касаясь использования RFID-ридеров, то тут возможно, как приобретение готовых, так и самодельных. В настоящее время в интернете размещено много способов изготовления таких ридеров.²

Обнаружить списание средств со счета возможно лишь только проверке баланса карты, либо с помощью услуги «мобильный банк» (СМС оповещение). В дальнейшем мошенники как правило переводят денежные средства с того счета, на который был осуществлено зачисление средств со счета жертвы на другие счета.

¹ Миронова Д.Д. Проблемы мошенничества с банковской картой и пути ее решения. [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: [http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=W&n=216847&fld=134&dst, свободно- Загл. с экрана. - Яз. рус. - \(Дата обращения: 14.11.2017\)](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=W&n=216847&fld=134&dst, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.11.2017))

² Потапова Н.Н. Некоторые особенности выявления и раскрытия бесконтактного мошенничества. Нижегородская академия МВД России [Электронный ресурс] // - Электрон. дан. - [М.]. - URL: [http://www.consultant.ru/cons/cgi/online.cgi?req=doc&baseAW&n=201204&fld=134&dst=1000000001,0&rnd=0.6731513152206969#0, свободно- Загл. с экрана. - Яз. рус. - \(Дата обращения: 14.10.2017\)](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&baseAW&n=201204&fld=134&dst=1000000001,0&rnd=0.6731513152206969#0, свободно- Загл. с экрана. - Яз. рус. - (Дата обращения: 14.10.2017))

Существуют несколько способов вывода средств:

- снять наличными с банкомата;
- перевод на другие счета;
- перевод на электронный кошелек (QIWI, «Яндекс.Деньги», WebMoney и др.)
- обмен на криптовалюту (биткоины и др.)

В заключении необходимо отметить следующее:

- установленный лимит в 1000 рублей невозможно изменить;
- защитить денежные средства, находящиеся на карте возможно только с помощью страхования;

В случае несанкционированного списания мошенниками средств со счета жертвы, банк не возвращает незаконно списанные денежные средства.

Таким образом, подведя итог вышесказанного можно сделать вывод, что данная услуга не обеспечивает достойной сохранности ваших денежных средств, но стоит надеется, что в дальнейшем банки устранят данную проблему в системе безопасности и пользователи смогут не беспокоиться о сохранности своих средств.

Горбанев Владимир Михайлович,

адъюнкт кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России;

Стукалов Вячеслав Владимирович,

доцент кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

О некоторых проблемах предупреждения и раскрытия мошенничеств, связанных с использованием средств сотовой связи

Оперативно-розыскная деятельность, осуществляемая сотрудниками подразделений уголовного розыска, представляет собой масштабную непрерывную работу по выявлению, предупреждению, пресечению и раскрытию преступлений, а также выявлению и установлению лиц, их подготавливающих, совершающих или совершивших; осуществлению розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших; добывание информации о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ, а также установление имущества, подлежащего конфискации¹.

¹ См.: Ст. 2 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

По нашему мнению, не требует подтверждения тот факт, что преступность шагает в ногу со временем и широко использует в своей деятельности все возможности достижений современной науки и техники. Совокупность свойств, которыми обладают в настоящее время средства сотовой связи, открывает широкие возможности для реализации мошенниками своих преступных замыслов с их использованием. Предупреждение и раскрытие мошенничеств, связанных с использованием средств сотовой связи, являются непосредственными задачами оперативных подразделений органов внутренних дел. Как отмечает министр внутренних дел Российской Федерации В.А. Колокольцев, «... особую актуальность в современных условиях приобретает защита имущественных интересов граждан от воров и мошенников. По распространённости и темпам роста совершаемые ими преступления намного опередили остальные виды противоправных деяний»¹.

Мошеннические действия рассматриваемого вида являются преступлениями новой формации, дистанционными, то есть для их совершения не надо вступать в непосредственный контакт с лицом, которое предполагается обмануть, ввести в заблуждение и как результат получить от него денежные средства. Как результат, преступники совершают данные мошенничества в максимально комфортных для себя условиях, а именно:

- используют средства сотовой связи, в том числе sim-карты (не зарегистрированные, либо зарегистрированные на подставных лиц или по украденным документам), недолгое время (от 10 до 30 дней), после чего их выбрасывают или уничтожают;

- находятся на многокилометровом расстоянии от потерпевших;

- не все потерпевшие обращаются в правоохранительные органы с заявлениями о совершенных в их отношении мошенничествах, связанных с использованием средств сотовой связи;

- находятся, как правило, вне досягаемости сотрудников подразделений уголовного розыска, которым, в силу выполнения своих должностных обязанностей, стало известно о таких мошенничествах;

- зная о способах действий и возможностях правоохранительных органов (даже в общих чертах) по предупреждению и раскрытию преступлений, а также по выявлению и установлению лиц, их подготавливающих, совершающих или совершивших, используют денежные средства, полученные от потерпевших (включая и сами способы получения этих денежных средств), с учетом этих знаний, максимально осторожно, избегая опасности быть задержанными с поличным и т.п.

¹ См.: Выступление министра внутренних дел Российской Федерации В.А. Колокольцева на расширенном заседании коллегии МВД России (15 марта 2016 года) // URL: <http://www.kremlin.ru/events/president/news/51515>. (дата обращения 28.10.2017 г).

Для предупреждения и раскрытия мошенничеств, связанных с использованием средств сотовой связи, сотрудниками оперативных подразделений используются и применяются различные мероприятия, силы, средства и методы, с присущей им определенной спецификой. Организация и тактика раскрытия мошенничеств, связанных с использованием средств сотовой связи, обусловлена наличием информации о характерных общих чертах, свойственных группе этих преступлений, таких как способы их совершения, личностей потерпевшего, преступника и ряда других обстоятельств¹. Поэтому данная специфика, а именно совокупность информационных данных о мошенничествах, связанных с использованием средств сотовой связи, находит свое отражение в оперативно-розыскной характеристике преступлений этого вида.

Основными элементами оперативно-розыскной характеристики мошенничеств, связанных с использованием средств сотовой связи, по нашему мнению, являются:

- структура и динамика этого вида преступлений;
- характеристика потерпевших от данных действий;
- характеристика лиц, совершающих данные преступные деяния;
- способы совершения рассматриваемых преступлений и ряд других.

Данная структура, на наш взгляд, наиболее полно и последовательно отражает сущность данного противоправного явления, что не может не послужить основой для рационального и правильного принятия решения руководителями оперативных подразделений о применении и использовании имеющихся сил, средств, методов, проведении необходимых мероприятий.

Таким образом, структура и динамика, характеристика потерпевших, характеристика лиц, совершающих данные преступные деяния, способы совершения рассматриваемых преступлений являются важными и значимыми элементами оперативно-розыскной характеристики мошенничеств, связанных с использованием средств сотовой связи, которая обладает значительной степенью информативности, позволяющей выдвигать версии в отношении, как обстоятельств совершения самого преступления, так и личностей потерпевшего и преступника, что, в свою очередь, может способствовать решению проблем по предупреждению и раскрытию этих мошенничеств.

¹ См.: Горбанев В.М. Оперативно-розыскная характеристика мошенничеств, связанных с использованием средств сотовой связи // Общество и право, 2016. – № 4 (58).

Горбунов Алексей Николаевич,
старший преподаватель кафедры оперативно-разыскной
деятельности в ОВД
Краснодарского университета МВД России

Основные источники угроз экстремизма в современной России

Актуальность проблемы по борьбе с экстремизмом не вызывает ни каких сомнений. Во всех своих проявлениях экстремизм носит агрессивный, подстрекательский, а не редко насильственный характер, связанный с террором. Он посягает на права и свободу граждан и подчас прямо на их жизнь, несет угрозу национальной безопасности, наиболее опасен и для общества и для государства. По мнению Президента Российской Федерации В.В. Путина, в последнее время участились случаи разжигания социальной, расовой, национальной розни, распространения идей фашизма. Эти крайне опасные явления в жизни нашего общества подрывают основы конституционного строя, общественную безопасность и государственную целостность Российской Федерации, ведут к попранию конституционных прав и свобод человека и гражданина¹.

Главенствующую роль в противодействии экстремизму занимает правовое регулирование указанной деятельности государства, что имеет первостепенную задачу по созданию новых, а так же конкретизации старых нормативно-правовых актов. Действующие в настоящее время нормативные правовые акты, регулирующие различные аспекты противодействия экстремизму, по справедливому мнению специалистов, требуют доработки, пояснений и полного переосмысления.

Современное законодательство в сфере противодействия экстремизму представлено двумя ярко выраженными нормативными актами: Указом Президента от 12.05.2009 года «О стратегии национальной безопасности РФ до 2020 года» и Федеральным законом № 114 от 25.07.2002 года «О противодействии экстремисткой деятельности».

В развитие положений стратегии национальной безопасности, была принята «Стратегия противодействия экстремизму в Российской Федерации до 2025 года»² (далее – Стратегия). Разработкой данной Стратегии занималось Министерство внутренних дел Российской Федерации совместно с другими министерствами и ведомствами, заинтересованными в решении этой проблемы.

Принятие Стратегии продиктовано повышением эффективности мер, принимаемых органами государственной власти, местного самоуправления и правоохранительных органов по противодействию экстремизму.

¹ Выступление Президента Российской Федерации В.В. Путина на Совете Безопасности Российской Федерации 20.11.2014 г.

² Утверждена Президентом РФ 28.11.2014 г., Пр-2753.

Стратегия занимает определенное место в иерархии нормативных правовых актов в сфере обеспечения национальной безопасности, а потому требует подробного изучения и анализа. Этим и обусловлена актуальность рассмотрения основных положений Стратегии противодействия экстремизму в Российской Федерации до 2025 года.

Учитывая, что анализируемая Стратегия утверждена в конце 2014 года, каких-либо исследований по ее основным положениям в специальной литературе нет. Имеются лишь отдельные комментарии специалистов, не содержащие комплексного взгляда на содержание Стратегии. Все это свидетельствует о том, что настоящее исследование основных положений Стратегии имеет новизну, а так же значимость как для дальнейших теоретических исследований правовых вопросов противодействия экстремизму в России.

Рассматривая источники угроз экстремизма в современной России, авторы Стратегии отмечают, что за последние годы увеличилось число внешних и внутренних экстремистских угроз. При этом к числу внешних угроз отнесены:

- поддержка иностранными государственными органами и организациями экстремистских проявлений в целях дестабилизации общественно-политической обстановки в Российской Федерации;
- деятельность международных экстремистских и террористических организаций, приверженных идеологии экстремизма.

По мнению А.Л. Сулейманова, рост международного экстремизма определяется следующими обстоятельствами:

- 1) общим ростом масштабов и активности политического экстремизма в большинстве регионов России;
- 2) вовлечением в этот процесс все более значительных слоев и групп населения;
- 3) широким применением особо опасных форм и методов политически мотивированного насилия¹.

Наряду с внешними угрозами Стратегией выделяются и внутренние, к числу которых относятся:

- экстремистская деятельность радикальных общественных, религиозных, неформальных объединений, некоммерческих организаций;
- экстремистская деятельность отдельных лиц.

Данные угрозы представляют особую опасность, ввиду тех специфических черт, которые они в себе несут. Люди, подвергающиеся давлению со сторон организаций экстремисткой направленности, поначалу могут и не понимать противоправность данной идеологии, и те цели, которые они

¹ Сулейманов А.Л. Влияние международного экстремизма на криминогенную ситуацию в регионах российской Федерации // Пробелы в российском законодательстве. Юридический журнал. № 6 / 2012. С.146.

преследуют. Вовлечение в экстремизм является не минутным делом и эффект от них формируется по истечению определенного времени. С каждым годом все большее и большее количество людей вступают в преступные организации в связи с нестабильностью современного общества; культурных, социальных и экономических сфер.

К наиболее опасным видам экстремизма Стратегия относит националистический, религиозный и политический экстремизм. При этом, как указывается в Стратегии, указанные виды экстремизма проявляются в возбуждении ненависти либо вражды по признакам пола, расовой, национальной, языковой, религиозной принадлежности или принадлежности к какой-либо социальной группе, в том числе путем распространения призывов к насильственным действиям, прежде всего через информационно-телекоммуникационные сети, включая сеть "Интернет", в вовлечении отдельных лиц в деятельность экстремистских организаций или групп, в проведении несогласованных акций, организации массовых беспорядков и совершении террористических актов.

Очевидно, – пишут В.А. Алещенков и В.Н. Шишилин, – что регионально-клановый и националистический экстремизм (и это видно наглядно на примере Северного Кавказа) имеет своим главным источником экономические факторы и причины: безработица, бедность населения, «демонстрационный эффект» жизненного уровня Москвы, пораженной вирусом коррупции и высокомерного потребительства. Очевидно, что данная социально-политическая модель ведет Россию в социальный тупик¹.

Действующее Российское федеральное законодательство не в полной мере способно противостоять политическому и религиозному экстремизму. До сих пор нет четкого определения понятий политического и религиозного экстремизма, что создает немало трудностей в борьбе с проявлениями экстремизма для всех органов государственной власти.

Отдельным источником угрозы экстремизма в Стратегии выделены информационно-телекоммуникационные сети, включая сеть «Интернет», которые стали основным средством коммуникации для экстремистских и террористических организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии.

По мнению сотрудников правоохранительных органов, сложность борьбы с экстремистами в сети «Интернет» заключается в том, что виртуальное пространство позволяет им оставаться анонимными. Кроме основных сайтов экстремисты обычно создают 2–3 так называемых «зеркала»,

¹ Алещенков В.А., Шишилин В.Н. Регионально-клановый и националистический экстремизм: проблемы территориальной целостности государства // Фундаментальные исследования. Вып. № 3-2 / 2012. С.466.

через которые их также можно посещать. Что касается социальных сетей, то здесь всё еще проще: сразу же после закрытия одного аккаунта экстремисты открывают другой.

В зависимости от вида преступлений экстремистской направленности сети «Интернет» могут быть использованы для:

- распространения экстремистских материалов (публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма и др.);

- обеспечения деятельности экстремистских сообществ, организаций (склонение, вербовка или иное вовлечение лиц в совершение преступлений экстремистской направленности, руководство сообществом, организацией, его частью, разработки планов, условий для совершения преступлений экстремистской направленности, связи, инструктажа участников и т.п.).

Информационно-телекоммуникационные сети, включая сеть "Интернет", стали основным средством коммуникации для экстремистских и террористических организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии. Используя мировую сеть Интернет, члены экстремистских движений активно вовлекают новых членов в свою деятельность, что приводит к обострению главным образом молодежного экстремизма. С помощью нее члены экстремистских групп получили возможность вступать в дискуссии, отстаивать свои взгляды главным образом, не раскрывая своих личностей.

С помощью Интернета они имеют реальную возможность влиять на разум людей и преподносить свои взгляды таким образом, что они кажутся действительным решением проблем современного общества. У них появился шанс распространять в глобальном масштабе экстремистские материалы, показывать все плюсы своих идеологий и вовлекать большое количество новых членов так скажем «не выходя из дома»

Интернет все чаще используется экстремистскими организациями для пропаганды своих идей. Результаты проведенного опроса студентов юридических факультетов показали, что 67% респондентов знают о существовании сайтов экстремистской направленности, а 2% их регулярно посещают. А ведь именно молодежь и подростки, в силу присущих возрасту психологических особенностей являются наиболее благоприятной средой для усвоения крайних взглядов.

Экстремизм в наше время носит открытый характер только в редких случаях, в основном он глубоко спрятан и адаптируется к современным условиям, главным образом через сеть Интернет. Теперь участникам экстремистских движений не составляет труда общаться со всеми членами организации в любом месте, имея при себе самый обычный смартфон с вы-

ходом в сеть Интернет и нет необходимости собираться вместе для решения той или иной задачи.

В глобальной сети Интернет члены экстремистских движений и групп преследуют несколько целей. Во-первых, это опубликования для всеобщего ознакомления своих радикальных программ, содержащих информацию о необходимости насильственного изменения конституционного строя России и нарушение ее целостности, а также пропаганду доминирования граждан по признакам их отношения к религии, расе, языковой принадлежности и т.д.

Во-вторых Интернет активно используется участниками экстремистских организаций для быстрого и без дополнительных затрат найти различные способы изготовления самодельных взрывчатых устройств, а также информацию по всем нужным аспектам осуществления преступлений экстремистской направленности.

В-третьих, данные организации используют Интернет для получения реальных доходов (через рекламу, трафики захождения на сайт и т.д.) и финансирование своей деятельности, либо для получения содействия в планировании, организации и совершении преступных действий.

Помимо рассмотренных выше основных угроз экстремизма в современной России Стратегия содержит и другие, не менее опасные проявления, требующие своего глубокого анализа, однако в силу ограниченного объема работы, проанализировать их не представляется возможным. К таким угрозам относятся:

- крайнее проявление экстремизма – терроризм, который основывается на экстремистской идеологии;
- экстремистская идеология, которая является основным компонентом, объединяющим членов экстремистских организаций, формирующим характер и направленность их деятельности, а также средством вовлечения в экстремистскую деятельность различных слоев населения;
- привлечение различных групп населения к участию в протестных акциях, в том числе несогласованных, которые впоследствии умышленно трансформируются в массовые беспорядки;
- проникновение из других государств радикальных течений ислама, проповедующих их исключительность и насильственные методы распространения;
- неконтролируемая (в том числе незаконная) миграция и недостаточно регулируемые на региональном и муниципальном уровнях миграционные процессы, зачастую нарушающие сложившийся в отдельных регионах и муниципальных образованиях этноконфессиональный баланс населения, и другие.

Подводя итог необходимо отметить, что противодействие экстремистской деятельности является приоритетным направлением государ-

ственной политики по защите общественной и государственной безопасности.

Стратегия противодействия экстремизму в Российской Федерации до 2025 года, принятая в развитие положений стратегии национальной безопасности, является важнейшим документом в сфере противодействия экстремизму, так как она раскрывает основные направления реализации данной деятельности, а также выделяет особо важные сферы для деятельности государства и общества по противодействию экстремизму.

Положения Стратегии еще предстоит детально исследовать и глубоко изучить в рамках противодействия экстремизму, и настоящая работа вносит определенный вклад в изучение этого важного документа.

Добросмыслов Андрей Эдуардович,
преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России;
Сафронов Андрей Алексеевич,
доцент кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

Информационное противоборство экстремизму и терроризму в сети Интернет

В настоящее время при всех положительных моментах повсеместного распространения сети Интернет, делающего общество более открытым и свободным, глобальная сеть стала одним из каналов распространения деструктивной идеологии, средством связи, координации проводимых экстремистских и террористических акций, инструментом вовлечения новых членов в ряды радикальных структур.

Следует отметить, что по данным Совета Безопасности Российской Федерации в глобальной сети насчитывается свыше 7,5 тыс. сайтов экстремистской направленности, из которых более 150 – русскоязычные.

При этом по российскому законодательству, как и в большинстве других стран, организации-провайдеры и владельцы сетевых ресурсов, предоставляющие услуги по размещению сайтов, фактически не несут ответственности за содержание размещаемой на них информации.

По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Особенно это касается предлагаемых глобальной сетью возможностей:

- свободного доступа;
- небольшие регулирование, цензура и другие формы государственного контроля или вовсе их отсутствие;

- потенциально огромная аудитория во всем мире;
- анонимность связи;
- быстрое движение информации;
- невысокая стоимость создания сайта и обслуживания присутствия в сети;
- мультимедийная среда: возможность комбинировать текст, графику, аудио и видео, возможность для пользователей загружать фильмы, песни, книги, постеры.

Таким образом, в современных условиях наиболее благоприятную среду для массового распространения радикальных идей и взглядов представляет глобальная информационно-телекоммуникационная компьютерная сеть Интернет.

Свободный доступ к информационным ресурсам сети Интернет при отсутствии достаточных правовых механизмов регулирования данной сферы предоставил отдельным лицам, организациям и объединениям, преследующим противоправные, в т. ч. экстремистские и террористические цели, новые возможности, прежде всего, для распространения информационно-пропагандистских материалов, планирование и координация нападений, вовлечения в свои ряды новых членов, ведение психологической войны (распространение дезинформации, угроз), сбор данных, сбор денежных средств и финансирование различных акций.

Как показывает практика, Интернет-среда и, в частности, социальные сети, активно используются для вербовки новых членов террористических организаций, а также для массового распространения экстремистской идеологии, где проводится анализ личной информации, вводимой пользователем при регистрации на сайте или в опросах, по которой можно определить его отношение к той или иной проблеме.

С пользователями, которые представляются наиболее заинтересованными в деятельности объединения или подходящими для выполнения какого-либо задания, устанавливается контакт. Кроме того, в социальных сетях «Одноклассники», «ВКонтакте» и других создаются закрытые сообщества, в которых распространяются материалы экстремистской направленности, участникам сообщаются сведения о месте и времени проведения акций и осуществляется координация деятельности экстремистских группировок.

Также, действия подобного характера ведутся в мессенджерах (WhatsApp, Viber, Телеграмм), разработанных для мобильных и иных платформ с поддержкой голосовой связи для мгновенного обмена текстовыми сообщениями.

Одним из немаловажных элементов противодействия экстремизму и терроризму в сети Интернет проведение на постоянной основе оперативных и мониторинговых мероприятий сети Интернет, блогосферы и других сетевых ресурсов, с целью выявления и идентификации лиц, распространяю-

щих в сети Интернет информацию и материалы, содержащие признаки призывов, оправданий терроризма и экстремизма, а также лиц, попавших под их влияние; оказанию адресного профилактического воздействия на категории лиц причастных к распространению идеологии терроризма, а также наиболее подверженных или уже подпавших под воздействие этой идеологии.

В целях контрпропаганды экстремистских, в том числе террористических проявлений, профилактики межэтнических и межконфессиональных конфликтов, необходимо размещение материалов в средствах массовой информации и коммуникации.

В 2017 году сотрудниками Центра по противодействию экстремизму ГУ МВД России по Краснодарскому краю в рамках проводимой работы по информационному противоборству экстремистским проявлениям, в открытых телекоммуникационных источниках выявлено 407 материалов экстремистского содержания, в том числе 183 материала, ранее внесенных в Федеральный список Минюста России по решениям судов.

В органы прокуратуры направлено 221 и Управление Роскомнадзора по ЮФО 110 материалов экстремистского содержания, выявленных в Интернете, для принятия мер прокурорского реагирования и ограничения доступа к данным Интернет-ресурсам.

Вместе с тем, сотрудники, осуществляющие информационное противоборство сталкиваются с такими проблемами как:

1. Отсутствие специальных компьютерных программ, позволяющих идентифицировать пользователя социальной сети, его место положение, ближайшие контакты и д.р;
2. Отсутствие специальных программ шифрующие ip-адреса сотрудников;
3. Отсутствие контроля систем мгновенного обмена текстовыми сообщениями для мобильных и иных платформ с поддержкой голосовой связи WhatsApp, Viber, Facebook, Twitter, Телеграмм и др.
4. Имеется возможность регистрации в сети Интернет гражданам по незарегистрированным в установленном порядке sim-картам;
5. Использование пользователями сети Интернет различных «Утилитов» для изменения ip-адресов, а так же полного их сокрытия;
6. Отсутствие технической возможности установления пользователей зарегистрированных на иностранных Интернет ресурсах.

В настоящее время проводится большая и многогранная работа по устранению угроз государству и обществу возникающих в сети Интернет, однако для реализации намеченных планов проведения информационного противоборства необходим новый подход, в котором необходимо:

- повышение квалификации сотрудников осуществляющих информационное противоборство в сети Интернет, с целью дальнейшего применения на практике в полном объеме возможностей 15 пункта, ч.1, 6 статьи

Федерального закон от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности» «Получение компьютерной информации» (п. 15 введен Федеральным законом от 06.07.2016 N 374-ФЗ);

- разработать единый механизм, позволяющий незамедлительно блокировать веб-сайты (включая иностранные), на которых размещаются призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, блокировки так называемого «анонимного серфинга» пользователя. Статья 15.3. («Порядок ограничения доступа к информации, распространяемой с нарушением закона») Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» дает право на блокировку таких веб-сайтов, однако единого механизма в ОВД нет;

- внедрение в ОВД специальных компьютерных программ позволяющих осуществлять мониторинг сети Интернет по ключевым словам, установление местоположение конкретного пользователя сети Интернет его идентификацию, в том числе и на иностранных Интернет ресурсах;

- внедрение компьютерных программ препятствующих осуществлению деятельности пользователей сети Интернет на территории Российской Федерации через различные программы, «Утилиты» позволяющие скрывать, изменять IP адрес технического устройства;

- ужесточение контроля над деятельностью компаний оказывающих телекоммуникационные услуги сотовой и фиксированной связи, проводного (FTTB) и беспроводного (Wi-Fi) высокоскоростного доступа в Интернет, IP-телевидения («Домашнее цифровое телевидение» и «Мобильное ТВ»).

Это далеко не весь перечень мероприятий требующих немедленной реализации, но воплощение хотя бы одного мероприятия позволит повысить деятельность оперативных служб ОВД в сфере информационного противоборства.

Зекох Анзаур Гилимович,
старший оперуполномоченный ОУР МО МВД России «Адыгейский»
(адыюнкт кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России)

Проблемы вовлечения лиц в деятельность экстремистских организаций

В настоящее время обострение межрелигиозных, межрасовых, межнациональных конфликтов, появление тенденций к усилению проявления ненависти и вражды относительно представителей иных религий, национальностей и рас является насущной проблемой в Российской Федерации. Вовлечение граждан в деятельность экстремистских организаций является

актуальной проблемой нашего общества и требует от правоохранительных органов принятия решительных мер, нацеленных на предупреждение и пресечение любых форм экстремизма.

Термин «экстремизм» происходит от лат. «extremus», что означает радикальный, крайний. В соответствии с Толковым словарем русского языка Ожегова С.И. и Шведовой Н.Ю. экстремизм – это приверженность в идеологии и политике крайним взглядам и деяниям¹.

К идейным предпосылкам зарождения экстремизма можно отнести появление и существование в обществе радикальных максималистских взглядов, проявляющихся в виде конкретных оценок и высказываний по религиозным, политическим, этническим и иным существенным вопросам общественной жизни. Экстремистский мотив закреплён в п. «е» ч. 1 ст. 63 УК РФ и заключается в совершении преступления по мотивам религиозной, национальной, расовой, идеологической или политической вражды либо ненависти или по мотивам вражды либо ненависти относительно какой-либо определенной социальной группы.

Правовые и организационные основы противодействия экстремистской деятельности определены Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»².

За ведение экстремистской деятельности в Российской Федерации предусмотрено наказание в виде уголовной ответственности.

Уголовная ответственность предусмотрена также за склонение, вербовку или другое вовлечение лица в деятельность экстремистской организации (ч. 1.1 ст. 282.2 УК РФ). Ввиду того, что данная норма включена в УК РФ относительно недавно (в 2014 г.)³, в настоящее время еще не выработана единообразная практика ее применения. Однако толкование ч. 1.1 ст. 282.2 УК РФ предоставлено в п. 15.1 Постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», в силу которого под вербовкой, склонением либо иным вовлечением лица в деятельность экстремистской организации понимаются умышленные действия по вовлечению определенного лица в такую деятельность, к примеру, путем подкупа, уговоров, угрозы, просьб либо убеждения (в том числе, произведенные при помощи распространения материалов через информационно-телекоммуникационные сети и размещения материалов на различных носителях), посредством поиска лиц и вовлечения

¹ Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. М., 1994. С. 896.

² Статья: Некоторые аспекты уголовной политики государства по противодействию экстремизму на современном этапе (Крупницкая В.И., Розумань И.В.) («Вестник Омской юридической академии», 2016, № 4);

³ Федеральный закон от 5 мая 2014 г. № 130-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс»

их в деятельность экстремистской организации или применения по отношению к ним физического воздействия¹.

Преступление по склонению, вербовке или иному вовлечению лица в деятельность экстремистской организации считается оконченным с момента совершения данных действий, вне зависимости от того, было ли фактически вовлечено лицо в деятельность экстремистского объединения².

По своей юридической природе действия по склонению, вербовке или иному вовлечению лица в деятельность экстремистской организации представляют собой подстрекательство к преступлению. В соответствии с общими положениями института соучастия, подстрекателем является лицо, которое склонило другое лицо к совершению преступления посредством угрозы, подкупа, уговора либо иным способом (ч. 4 ст. 33 УК РФ). Подстрекательство к указанному преступному деянию предполагает действия, направленные на формирование у лица добровольного желания принять участие в деятельности экстремистской организации посредством убеждения в правильности существующих в сообществе взглядов, при помощи уговоров, призыва к религиозным чувствам и т.д. Подстрекательство также охватывает применение физического воздействия, угроз и других способов вовлечения лица в деятельность такой организации³.

В связи с недовольством положением дел в стране и социально-экономическими трудностями, граждане, особенно молодые люди в возрасте до 30 лет, легко вовлекаются в экстремистскую деятельность: идеологи экстремистских организаций оказывают на них воздействие для формирования убеждений, позволяющих рассматривать экстремистские действия как способ решения межрелигиозных, межнациональных, социально-политических и других конфликтов, а также как способ самореализации⁴.

Значительную опасность для российского общества и государства представляют сайты в сети Интернет, распространяющие идеологию экстремизма, так как посредством Интернет-ресурсов осуществляется вовлечение лиц в деятельность экстремистских организаций. Для вовлечения лиц в деятельность экстремистских организаций идеологами экстремизма используются все популярные ресурсы и социальные сети: «Facebook», «ВКонтакте», «Youtube», «Twitter», «Instagram». При этом используются

¹ Статья: Организация экстремистского сообщества: проблемы квалификации (Клименко Ю.А.) ("Lex russica", 2017, № 3)

² Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 03.11.2016) «О судебной практике по уголовным делам о преступлениях экстремистской направленности»

³ «Справка по итогам изучения судебной практики Ульяновской области по уголовным делам о преступлениях террористической и экстремистской направленности» (подготовлена судебной коллегией по уголовным делам Ульяновского областного суда)

⁴ Власов В. И. Экстремизм, терроризм, сепаратизм: политико-правовое осмысление в условиях глобализации : лекция / В. И. Власов ; Рос. акад. гос. службы при Президенте Рос. Федерации. – Москва: Издательство РАГС, 2009

все возможности социальных сетей: «репосты», массовые рассылки, размещение документов, фотографий, музыкальных и видеоматериалов.

Вербовщики используют индивидуальный подход, применяя сведения, которую они могут найти в сети о лицах, прямо или косвенно интересующихся деятельностью экстремистских организаций. При этом используются узнаваемые слоганы, символы и стиль. У людей формируется неверное представление о некой социальной группе, отличной от иных общностей целостностью знаний о происходящем вокруг. Символы и слоганы подаются посредством популярных среди молодых людей форматов: мемов, демотиваторов, подражаний и т.д. Инструментами воздействия являются технологии манипуляции: формирование и развитие идеологии «свой-чужой», создание образа «врага», воспитание в людях чувства превосходства одной национальности над другой.

По мнению Н. С. Седых¹, использование экстремистами сети Интернет позволяет осуществлять «управление восприятием»: идеологи экстремизма могут позиционировать себя как «добропорядочных, религиозных граждан, ведущих просветительную деятельность». Целенаправленное «управление восприятием» позволяет идеологам экстремистских организаций убедить людей в их личной заинтересованности в тех или иных идеологиях, взглядах и целях, завербовать противников в сторонники, расходуя имеющиеся ресурсы по минимуму. Так, благодаря сети Интернет праворадикальное движение «Misanthropic Division» в настоящее время имеет 18 автономных ячеек по всему миру, в том числе в странах Северной Америки и Западной Европы.

Важно заметить, что при помощи сети Интернет гражданам показываются сцены пыток и убийств мирных жителей и военнослужащих, проводится политика масштабного информационного террора. В качестве примера можно привести многочисленные случаи распространения видеосюжетов, демонстрирующих убийства иностранных граждан в Ираке. Данные сцены «казни» вызвали бурный общественный резонанс.

В 2014 году в Южном федеральном университете среди студентов проводился социологический опрос на тему «Экстремизм в сети Интернет». В соответствии с данными опроса, молодые люди не интересуются экстремизмом: лишь 3% из них посещали сайты экстремистской направленности, 1% заходили на сайты, посвященные противодействию экстремизму.

Молодые люди придерживаются того мнения, что под воздействие экстремистской пропаганды в Интернете попадают психологически слабые люди, подверженные чужому влиянию (29%), лица с психическими забо-

¹ Седых Н. С. Социально-психологические особенности пропаганды экстремизма и терроризма посредством интернета // Электронная версия журнала «Социальная психология и общество», № 2/2013;

леваниями (16%), дети и женщины (9%), а также лица с несформированными жизненными принципами (8%).

Опрошенные студенты уверены, что наиболее эффективным способом пропаганды экстремистской деятельности в сети Интернет являются видеоролики (50% опрошенных), 19% считают, что вербовать в экстремистские организации могут на в блогах или на форумах.

В Стратегии противодействия экстремизму в РФ до 2025, информационно-коммуникационные сети, включая Интернет, признаны одними из основных источников угрозы экстремизма в России¹.

В части стратегии о направлениях и задачах государственной политики в области противодействия экстремизму несколько пунктов посвящено пресечению деятельности экстремистских организаций (а также экстремистской направленности в целом) в сети Интернет².

Как отмечали на заседании Совета Безопасности РФ в 2014 году, важнейшей задачей указанной стратегии противодействия экстремизму является формирование государственной системы мониторинга не только телекоммуникационных сетей, но и информационного поля в целом. При этом директор компании «Ашманов и партнеры» Игорь Ашманов считает, что главный упор в мониторинге необходимо сделать на социальных сетях. Игорь Ашманов также пояснил: «Как легко догадаться, следующий кандидат на «майдан» и гражданскую войну – это мы. Об этом наши государственные деятели говорят абсолютно прямо. И подобные действия сейчас организуются с помощью социальных сетей. Поэтому первое, что необходимо сделать, – это собственно мониторинг, то есть анализ, что пишут. Второе – надо уметь с этим бороться. Это возможно с помощью ботов и других средств зашумления либо просто через перекрытие канала»³. Но как сопоставить данный контроль с незыблемыми конституционными правами граждан пока неясно.

Проведение мониторинга телекоммуникационных сетей однозначно является правильным решением, однако анализ социальных сетей не всегда приводит к верному результату. В социальные сети ежесекундно поступает колоссальный объем информации, в связи с чем сведения в «репостах» и блогах с оттенком, например, национальной неприязни, не всегда означают, что лица, опубликовавшие такие сведения, испытывают чувство ненависти по отношению к лицам иных национальностей.

Для пресечения вовлечению лиц в деятельность экстремистских организаций, необходимо принятие профилактических мер. Можно выделить

¹ «Стратегия противодействия экстремизму в Российской Федерации до 2025 года» (утв. Президентом РФ 28.11.2014 № Пр-2753).

² Тарасенкова А.Н. «Интернет: правовые аспекты безопасного использования» «Российская газета», 2017 выпуск 2.

³ «Совет безопасности Колокольцева» // <http://www.gazeta.ru>. 21.11.2014.

следующие меры профилактики по противодействию вовлечения лиц в деятельность экстремистских организаций:

- анализ и контроль данных в сети Интернет для выявления и блокирования пропаганды идеологов экстремизма;
- предоставление возможности пользователям сети Интернет подключиться к процессу обнаружения противоправного контента и его блокировки;
- разработка методических пособий по информационному противодействию экстремизму, легких для восприятия и интересных для молодежи;
- ведение разъяснительной работы с гражданами для раскрытия подлинной идеологии экстремизма, формирование стойкого неприятия обществом идей насилия;
- привлечение граждан к участию в противодействии экстремизму.

Указанные меры профилактики по противодействию вовлечения лиц в деятельность экстремистских организаций будут более эффективными, если сформировать четкие и ясные для понимания граждан цели:

- формирование условий для снижения социальной напряженности, агрессии и экстремистской активности;
- создание условий для развития социально-ответственной, толерантной, патриотичной, успешной личности;
- формирование альтернативных способов реализации социальной активности молодых людей: развитие позитивных молодежных субкультур, общественных движений, групп и объединений.

В заключение хотелось бы отметить, что, несмотря на возложение обязанности по защите общества от противоправной деятельности экстремистских организаций на государство, каждый член нашего общества должен понимать, что такое экстремизм, с какой целью идеологи экстремизма вовлекают граждан в деятельность экстремистских организаций, какие последствия может иметь экстремистская деятельность, осознавать опасность данного явления для государства и людей, проживающих в нем.

Безусловно, инициатива по противодействию экстремистской деятельности должна исходить от государства, но реализация данного противостояния должна всецело поддерживаться обществом.

Иванов Святослав Игоревич,
начальник кафедры оперативно-разыскной деятельности
и специальной техники Крымского филиала
Краснодарского университета МВД России,
кандидат юридических наук

Отдельные направления совершенствования оперативно-розыскной деятельности органов внутренних дел в современных условиях

Оперативно-розыскная деятельность по своей сути является деятельностью информационной, целью которой является добывание информации, способствующей решению задач, определенных в статье 2 Федерального закона «Об оперативно-розыскной деятельности».¹ В этой связи нельзя не обратить внимание на интернет-пространство, где на сегодняшний день сосредоточено огромное количество информации совершенно различного характера. Кроме того, Интернет все чаще становится и местом совершения преступления, и средством совершения преступления. Происходящие процессы относятся к компетенции различных оперативных подразделений органов внутренних дел. И эти тенденции имеют динамику к постоянному увеличению и требуют повышенного внимания со стороны оперативных подразделений. Процесс оперативно-розыскного мониторинга состоит из сменяющих друг друга фаз, а именно: сбора общей информации о среде функционирования; выявления информации о криминогенной обстановке и объекте оперативного внимания; поиска информации об объектах оперативного внимания в уголовно-активной и криминогенной среде с целью выявления тенденций развития преступности; поиска первичной оперативно-розыскной информации о конкретных преступлениях; сбора и оценки информации о силах и средствах правоохранительных органов; анализа результативности противодействия преступности; изучение общественного мнения о состоянии среды функционирования, криминогенной ситуации, результативности деятельности правоохранительных органов; анализа и оценки оперативной обстановки; прогнозирование ее развития и тенденций.² Поскольку среда, в которой все это должно происходить является не реальной, а виртуальной, то законодательной, научной, теоретической и практической разработки требует целый пласт вопросов оперативно-розыскной деятельности.

¹ Об оперативно-розыскной деятельности: федеральный закон Российской Федерации от 12.08.1995 № 144-ФЗ. – Доступ из СПС «КосультантПлюс».

² Пестрецов М.А. Противодействие преступным посягательствам на жилище граждан (на примере Республики Крым) / М.А. Пестрецов. – Краснодар: Краснодарский университет МВД России, 2017. – С.82.

Требуется всестороннего изучения такое понятие как, оперативная обстановка в сети для полного понимания условий интернет реальности в которой предстоит действовать.

Сам поиск, анализ, обработка, проверка информации в киберпространстве

требует разработки принципиально новых, по сравнению с имеющимися, подходов к проведению оперативно-розыскных мероприятий. Речь идет не только о проведении получения компьютерной информации и снятия информации с технических каналов связи, но и о проведении таких оперативно-розыскных мероприятиях, как опрос, наведение справок, сбор образцов для сравнительного исследования, обследование и др. Все они требуют адаптации к применению в новой среде, а возможно потребуются и разработка новых видов оперативно-розыскных мероприятий.

Как известно, корыстные преступления нацелены на извлечение материальной выгоды от совершения преступления, а когда эта выгода имеет выражение в незаконном присвоении или использовании криптовалют, то и мероприятия позволяющие выявлять, предупреждать, пресекать, раскрывать такие преступления должны быть соответствующими.

С одной стороны, старые добрые методы оперативно-розыскной деятельности и методы защиты информации в киберпространстве не имеют того успеха в решении поставленных перед ними задач, как раньше, с другой стороны – попытка решить возникающую проблему только за счет глубоко технических знаний, без адаптации к новым условиям имеющихся методов и способов работы, также будет малоэффективной. Развитие ОРД видится нам именно в интеграции технических и специальных знаний.

Изменившиеся условия проведения ОРМ, в свою очередь, изменяют и тактику ОРД. Перспективным считаем научную разработку такой темы как конспирация в интернет-пространстве, поскольку требования к ней в условиях сети являются отличными от требований в реальной жизни.

Интересным с точки зрения научного обсуждения является возможность использования конфиденентов в сети, а также появление такой новой категории конфиденентов, как сетевой конфиденент.

Важным является изучение правовых аспектов использования в киберпространстве содействия граждан органам, осуществляющим оперативно-розыскную деятельность.

Принципиальное значение приобретает возможность практически молниеносной обработки огромного количества исходных данных с целью получения искомой информации. Это продиктовано спецификой существования киберпространства и тех аспектов, которые имеют соприкосновения с этим пространством и совершающимися преступлениями.

Тенденции развития рынка различных умных вещей или так называемых гаджетов позволяет предположить, что возможность доступа к сети Интернет будет только увеличиваться, и этот доступ будет охватывать все

большие и большие сферы нашей жизни. Технические возможности самих гаджетов уже на сегодняшний день соответствуют техническим возможностям специальной техники разведслужб конца прошлого века, и это развитие идет семимильными шагами. Многофункциональные возможности умных вещей позволяют собирать колоссальные массивы информации, доступ к которой как законный, так и криминальный, имеется через сеть Интернет.

Вероятно, в ближайшем времени появятся и новые способы совершения различных преступлений в сети. Отдельные действия потребуют специальной юридической квалификации. Это потребует от нас знаний их оперативно-розыскной характеристики.

Очевидно, что обозначенная в докладе проблема должна решаться комплексно. Она касается законодательного урегулирования отдельных вопросов правоотношений в киберпространстве во многих отраслях права. Все это, в свою очередь, заставляет нас с вами задуматься о возможностях совершенствования нашей работы. Очень важно сейчас не утратить принцип наступательности и не оказаться в итоге далеко позади уходящего вдалека поезда. Уже сегодня надо быть интеллектуально готовым к решению задач будущего. Безусловно, это связано и с подготовкой будущих оперативных сотрудников, которым придется работать в условиях, о которых идет речь в докладе.

Кибатов Максим Сергеевич,
курсант Казанского юридического Института МВД России;
Музеев Айдар Иршатович,
доцент кафедры оперативно-розыскной деятельности
Казанского юридического института МВД России,
кандидат юридических наук

**Использование специального программного обеспечения
в оперативно-розыскной деятельности по противодействию
преступлений, совершаемых с использованием
компьютерных технологий**

За последнее десятилетие резко возросло количество преступлений в сфере и с применением высоких технологий. Только за первое полугодие 2015 года их количество выросло на 67% по сравнению с аналогичным периодом 2014 года. При этом, согласно статистике ГИАЦ МВД, количество расследованных уголовных дел в этой сфере год за годом снижается. К примеру, в 2010 г. Расследовано 6142 преступления, а в 2015 г. – 2470.

Эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что ос-

новными преступными деяниями, образующими рынок киберпреступности в России, являются:

- 1) мошенничество в системах интернет-банкинга;
- 2) фишинг;
- 3) хищение электронных денег;
- 4) услуги обналичивания иных нелегальных доходов;
- 5) спам (информация о медикаментах и различной контрафактной продукции, поддельном программном обеспечении, сфере услуг, образования, туризма и др.);
- 6) продажа трафика;
- 7) продажа эксплойтов;
- 8) продажа загрузок;
- 9) анонимизация;
- 10) DDoS-атаки.¹

Среди наиболее тяжело раскрываемых преступлений с применением высоких технологий можно выделить мошенничество, хищение денежных средств без прямого финансового контакта преступника с потерпевшим. Согласно официальной статистике, в 2014 году возбуждено 995 уголовных дел, что на 43,6% больше, чем в 2013. По данным статистики ГИАЦ МВД за 2015 год, на данный вид преступлений приходится 31% от общего числа правонарушений в сфере высоких технологий.

Сложность раскрытия такого вида правонарушений заключается в умелой анонимизации преступников. Получение денег злоумышленниками в этом случае происходит через посредников, занимающихся обналичиванием незаконно добытых средств. В этом случае трудно определить не только мошенника, но и обнальщика, так как большинство денежных операций происходит в сети Интернет с использованием обезличенных виртуальных валют. Согласно отчету FATF наиболее востребованным видом криптовалюты является Bitcoin, разработанный неизвестным для широкой общественности программистом (или группой программистов), выступающим под псевдонимом Satoshi Nakamoto, под авторством которого в ноябре 2008 г. была опубликована «Белая книга» с описанием механизма функционирования Bitcoin и его протокола. Bitcoin – это децентрализованная P2P платежная сеть, обслуживаемая ее пользователями, функционирующая без органов управления и посредников на фоне отсутствия централизованного контроля. В основе сети Bitcoin лежит публичный реестр (Blockchain, или «цепочка блоков»), в котором хранится информация обо всех произведенных транзакциях пользователей сети между собой и тем самым подтверждается или опровергается факт проведения той или иной

¹ Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации. // Юридическая наука и правоохранительная практика 1 (35), / К.Н. Евдокимов. – Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, 2016, С. 18

транзакции. В свою очередь, подлинность каждой транзакции защищена электронными подписями в соответствии с использованными в транзакции адресами, что позволяет пользователям иметь полный контроль над процессом передачи Bitcoin со своих Bitcoin адресов получателям.¹

Также ни одно серьезное преступление в сфере высоких технологий не проходит без использования средств анонимизации. Анонимизация чаще всего заключается в изменении свойств сетевого профиля субъекта с целью обеспечения их несвязности с пользователем, либо же с целью использования более распространенных значений некоторых свойств.² Это обстоятельство значительно затрудняет, а иногда делает невозможным установление реального IP-адреса киберпреступника. Одним из наиболее распространенных и эффективных способов, маскирующих реальное местоположение пользователя сети, является использование браузера TOR. Он находится в свободном доступе для скачивания и установки. Скачав его, любой человек может замаскировать свой IP-адрес как минимум через 5 звеньев. Вышеуказанный браузер используется в основном рядовыми пользователями сети «глубокого Интернета» для получения доступа к сайтам, недоступным в обычных браузерах с доменными именами .onion. Основная цель массового использования Тор'a – покупка запрещенных законодательством товаров, таких как: наркотики, поддельные документы, оружие и т.д. Он так же подходит для осуществления профессиональной преступной деятельности.

Использование данного ПО в 99% случаев делает невозможным вычислить преступника путем отправки запросов интернет-провайдерам и хостинг-компаниям. В основном это обусловлено большим количеством времени, уходящим на расшифровку цепи IP-адресов, поскольку они становятся известны последовательно отправке запросов. Более того, отправка запросов в большинстве случаев не эффективна, поскольку владельцы серверов, через которых проходит интернет-трафик злоумышленника, как правило, находятся на территории и в правовом поле иностранного государства. Таким образом получение компьютерной информации путем последовательной отправки запросов владельцам серверов, через которые проходил трафик злоумышленника не дает результатов, ведущих к идентификации мошенников при использовании ими браузера.

Для большей надежности преступники работают с TOR'ом через соединения VPN, шифрующие интернет-трафик. VPN (англ. Virtual Private Network — виртуальная частная сеть). VPN – это обобщённое название

¹ Батоев В. Б. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России / В. Б. Батоев, В.В. Семенчук. – М. 2017. № 2 (42), С. 11.

² Тюрин К.А. Алгоритм вероятностной идентификации пользователей сетей / К.А. Тюрин, Н.В. Болдырихин. Ростов-на-Дону: Издательство Донского государственного технического университета, 2016, С. 84.

технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии. В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

VPN-туннель – это виртуальное зашифрованное стойким алгоритмом соединение. Наглядно, его можно представить в виде непрозрачной трубы, а еще лучше такого тоннеля, один конец которого упирается в компьютер рядового пользователя, а второй в специализированный сервер, находящийся, как правило, в удалении или даже в другой стране. Современные виды VPN-подключения:

- PPTP (англ. Point-to-point tunneling protocol);
- OpenVPN;
- L2TP (англ. Layer 2 Tunneling Protocol).

PPTP (Point-to-point tunneling protocol) – это такой туннельный протокол типа «точка-точка», который позволяет компьютеру пользователя устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Этот протокол (PPTP) стал известен, потому что, это первый VPN – протокол, который поддерживала корпорация Microsoft. Все версии Windows, начиная с Windows 95 OSR2, уже включают в свой состав PPTP-клиент. Это самый известный и простой в настройке вариант подключения к VPN-сервису. Но, как говорится, есть здесь и отрицательный момент: многие интернет-провайдеры блокируют работу PPTP подключений.

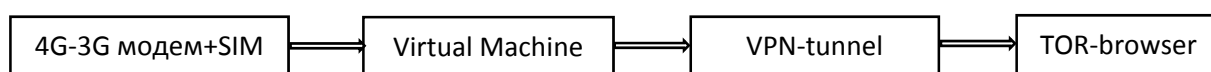
OpenVPN – это свободная реализация технологии Виртуальной Частной Сети (VPN) с открытым исходным кодом для создания зашифрованных каналов вида «точка-точка» или сервер-клиенты между компьютерами. Она может устанавливать соединения между компьютерами, которые находятся за NAT-firewall без необходимости изменения его настроек. Но использование, этой технологии потребует установки дополнительного программного обеспечения для всех операционных систем.

L2TP (Layer 2 Tunneling Protocol) – это сетевой протокол туннелирования канального уровня, сочетающий в себе протокол L2F (layer 2 Forwarding), разработанный компанией Cisco, и протокол корпорацией Microsoft. Позволяет создавать VPN с заданными приоритетами доступа, однако не содержит в себе средств шифрования и механизмов аутентификации (для создания защищённой VPN и его используют совместно с

IPSec). По отзывам экспертов, является наиболее защищенным вариантом VPN подключения, несмотря на трудность его настройки.¹

Во избежание идентификации по личным аккаунтам в почтовых сервисах и социальных сетях, злоумышленники работают через виртуальную машину. И TOR и программы для подключения через VPN-туннели устанавливаются на чистую Windows, которая работает на основе программ VMware и VirtualBox. Такая комбинация действий исключает возможность подключений злоумышленника через IP-адреса, используемые для преступных действий.

Заканчивается цепочка анонимизации использованием 3G или 4G модема и симок, купленных на сайтах объявлений у неизвестных лиц. Схематично она выглядит следующим образом:



При использовании вышеуказанной схемы вычислить преступника путем наведения справок практически не представляется возможным.

Один из вариантов решения проблемы деанонимизации преступника – разработка и использование оперативными подразделениями специального программного обеспечения, направленного на вычисление реальных IP, MAC адресов преступников, идентификации личности преступника по содержимому его компьютера.

Данная программа работает по типу троян-вируса в оболочке картинки, архива, файла-документа и т.д. Программа инициирует сбор информации об аппаратном и программном обеспечении с последующей записью её в отдельный файл. После чего данный файл отправляется по заранее определенному адресу. Обычным способом отследить отправку этой информации затруднительно, поскольку отправляемый трафик пользователя сети интернет не подотчетен провайдеру. Это повышает эффективность использования данного ПО.

Использование программы может проходить в 4 этапа:

- 1) Внедрение программы в файл-ловушку. При открытии файла, программа внедряется в ПК преступника.
- 2) Отправка файла злоумышленнику. Процесс должен проходить легитимировано, от имени потенциальной жертвы, либо другим способом.
- 3) Внедрение программы в ПК преступника.
- 4) Получение данных об аппаратном и программном обеспечении злоумышленника.

Исходя из вышеизложенного можно заключить, что применение использования данного программного обеспечения в оперативно-розыскной

¹ Артамонов В.А. Использование VPN. // МНОО «Международная академия информационных технологий» (ООН) / Артамонов В.А., Артамонова Е.В. 2016, С. 3

деятельность ОВД может быть эффективно при идентификации преступников в сети Интернет. Вместе с тем необходимо, с одной стороны, нормативное правовое закрепление данного действия как допустимое средство борьбы с киберпреступностью, а с другой – разработка для правоохранительных органов соответствующего сертифицированного программного обеспечения. Иначе говоря, как юридический, так и технический аспекты в данного вопроса требуют детальной проработки.

Киселев Сергей Сергеевич,
старший преподаватель кафедры уголовного права и криминологии
Краснодарского университета МВД России,
кандидат юридических наук;
Белый Андрей Григорьевич,
заместитель начальника кафедры ОРД в ОВД
Краснодарского университета МВД России
кандидат юридических наук, доцент

Угрозообразующие факторы экстремистских и террористических проявлений на Северном Кавказе

В 2017 году на территории Северо-Кавказского федерального округа основными угрозообразующими факторами признаются:

1. Участие выходцев из субъектов РФ СК ФО в боевых действиях на территории ближневосточных государств, что создает предпосылки для последующего формирования из них ядра вооруженного бандподполья, налаживания каналов получения финансовых и материальных ресурсов.

Так, в ГУГТЭ МВД России из МИД России поступила информация в отношении четырех граждан Российской Федерации, задержанных 07.12.2016 правоохранительными органами Турецкой Республики в Уезде Тарсус при попытке пересечения турецко-сирийской границы. Из них трое были уроженцами Чеченской Республики (Саламханов Х.Х. 23.08.1996 г.р., Мурадов А.Р. 08.09.1990 г.р. и Мааев Ш.Т. 16.09.1996 г.р.), а четвертый – уроженцем республики Дагестан (Шейхов М.Г., 22.09.1995 г.р.). У задержанных имелись при себе поддельные удостоверения личности, выдаваемые в Турции сирийским беженцам. На территорию Сирии они ехали по приглашению неустановленного лица, с которым поддерживали общение посредством сети Интернет.

Ситуация двоякая. С одной стороны, как в 2016 г. заявил заместитель главы Махачкалинского комитета безопасности, Мухтар Эфендиев «Без них (террористов присоединившихся к джихаду в Сирии) жизнь в СК ФО возвращается в нормальное русло». А с другой стороны, при укреплении позиций России, ИГ постепенно теряет влияние, а с ним и территории на

Ближнем Востоке, что чревато возвращением российских боевиков на территорию округа и возрастанием радикальных угроз.

2. Сложная социально-экономическая ситуация, характеризующаяся объективными и субъективными причинами, низким уровнем жизни значительной части населения округа, безработицей. Не смотря на принятую в 2014 году государственную программу «Развития СК ФО на период до 2025 года»¹, крайне остро социально-экономические проблемы до сих пор стоят в Республике Северная Осетия-Алания и Республике Дагестан. Это является почвой для вовлечения в преступную сферу безработных, граждан с низким уровнем материальных доходов. Несмотря на принимаемые меры, Республика Дагестан остается одним из наиболее трудоизбыточных регионов Российской Федерации, имеет место опережающий рост численности трудовых ресурсов по сравнению с количеством вновь создаваемых рабочих мест. Наибольшую опасность при этом представляет втягивание в экстремистскую деятельность незанятой молодёжи.

По уровню материального благосостояния населения Дагестан занимает одно из последних мест среди субъектов РФ. Среднемесячная заработная плата по республике составляет менее 15 тысяч рублей и остается самой низкой по СК ФО. Официальная численность безработных в республике составляет более 145 тысяч человек (11% трудоспособного населения), по некоторым экспертным оценкам до 70% трудоспособного населения Дагестана не занято в общественном производстве. Кризисные явления в экономике и социальной сфере привели к значительному ухудшению криминогенной ситуации, в общем числе выявленных лиц, совершивших преступления, доля трудоспособных, нигде не работающих и не учащихся, составила 82%².

Одним из наиболее действенных рычагов воздействия, недовольство сложной жизненной ситуацией выступает и при целенаправленной идеологической обработке населения РСО-Алания (в первую очередь – молодежи). Данная проблема наиболее остро стоит в Моздокском, а также в Пригородном, Правобережном и Ирафском районах.

3. Латентно сохраняющиеся межнациональные конфликты и трения на межнациональной почве.

В настоящее время в округе имеют место следующие проблемные зоны: приграничье РСО-А и РИ, приграничье ЧР и РИ (спор о принадлежности части территорий Сунженского района РИ (5000 га), оспариваемых Чеченской Республикой, приграничье ЧР и РД (спор вокруг Новолакского

¹ Об утверждении государственной программы Российской Федерации «Развитие Северо-Кавказского федерального округа» на период до 2025 года: постановление Правительства РФ от 15 апреля 2014 г. № 309. Доступ из СПС «КонсультантПлюс».

² Справка о состоянии оперативной обстановки в Республике Дагестан и принятых мерах в сфере противодействия экстремизму и терроризму за 12 месяцев 2016 г. - С. 8.

и части территорий Хасавюртовского районов РД, входивших до 1944 года в состав ЧИАССР), восточные районы Ставропольского края (конфликт между русским, ногойским и даргинским населением), территория КБР (конфликт по поводу так называемых «межселенных территорий»), территория КЧР (противостояние между элитами карачаевского, черкесского и абазинского этносов по поводу приоритетов в экономической жизни в республике).

Следует также подчеркнуть сложные миграционные процессы (в последние годы изменилась этническая структура населения так называемых «традиционно славянских» районов КБР, где наблюдается значительный приток турок-месхетинцев), и «бытовой национализм» со стороны представителей деструктивно настроенной молодежи Республики Ингушетия, пытающихся искусственно перевести хулиганские действия и общеуголовные преступления, совершенные на бытовой почве, на межнациональные и межконфессиональные «рельсы».

4. Деструктивная деятельность ряда иностранных государств, международных и российских некоммерческих организаций, в том числе правозащитной направленности, по дискредитации российских органов власти и управления в глазах международной общественности и местного населения.

Наибольшего внимания требует к себе ситуация в Пригородном районе РСО-Алания, в местах с компактным проживанием лиц ингушской и осетинской национальностей и Моздокском районе. На развитие оперативной обстановки в Моздокском районе существенное влияние оказывает наличие на территории района ряда мусульманских общин и диаспор, которые могут быть использованы религиозными эмиссарами в целях распространения религиозного экстремизма и иных деструктивных действий, направленных на дестабилизацию общественно-политической обстановки.

Опасение вызывает деятельность мононациональных общественных организаций КБР и КЧР в рамках так называемого «адыго-черкесского фактора», предпринимающих усилия с целью принудить правительство России признать «геноцид адыгов в годы Кавказской войны XIX века».

При этом деятельность адыго-черкесских моноэтнических организаций и движений преследует следующие основные цели:

- создание на территории Республики Адыгея, Карачаево-Черкесской Республики, Кабардино-Балкарской Республики, части территории Краснодарского и Ставропольского краев, единого суперсубъекта («Великой Черкесии») с последующим его выходом из состава Российской Федерации;
- принуждение государственных структур Российской Федерации к официальному признанию так называемого «геноцида адыгов» в годы Кавказской войны XIX века, с последующей выплатой крупных денежных сумм потомкам пострадавших;

- организация массовой репатриации этнических адыгов, потомков мухаджиров XIX века из Турции, Сирии, Иордании и других мест компактного проживания на историческую родину.

Идеологической и правовой базой для деятельности деструктивных адыгских общественных организаций и объединений выступает Постановление Верховного Совета Кабардино-Балкарской ССР от 7 февраля 1992 г. № 977- XII-V «Об осуждении геноцида адыгов (черкесов) в годы русско-кавказской войны», резолюция парламента Республики Грузия от 20 мая 2011 года о признании геноцида черкесского народа, основанная на научно-историческом заключении, представленным профессором Тбилисского государственного университета Мерабом Чухуа.

5. Деятельность бандподполья, объединенного в так называемый «Вилаят Кавказ Исламского государства».

Целью которого, с 2014 г. является создание так называемого «независимого исламского государства «Имарат Кавказ»». Члены бандподполья, продолжают преступную деятельность, направленную на физическое устранение представителей государственных и правоохранительных органов, военнослужащих, а также религиозных деятелей и рядовых граждан. При этом сохраняется вероятность совершения диверсий на объектах транспортно-энергетического комплекса, а также в местах массового скопления людей.

6. Активное распространение радикальной и экстремистской идеологии, инициированное зарубежными исламистскими центрами.

В последние годы наиболее остро эта проблема стоит на территории Республики Дагестан. В сети Интернет, в социальных сетях ежедневно размещаются призывы к осуществлению экстремистской деятельности, призывы к осуществлению террористической деятельности, либо оправданию идеологии и практики терроризма, а также имеют место факты, направленные на возбуждение национальной, религиозной или расовой ненависти.

Ежегодно Центрами по противодействию экстремизму органов внутренних дел, дислоцированных на территории субъектов СК ФО, в процессе мониторинга сети Интернет выявляется более тысячи источников информации, содержащих материалы с признаками идеологии экстремизма.

7. Вербовочная деятельность международных террористических организаций.

Поиск потенциальных кандидатов, как правило, осуществляется на форумах, блогах и киберсообществах соответствующей направленности, интересующей членов экстремистских и террористических организаций. Путем мониторинга интернет-ресурсов и прочтения содержания переписки вербовщиками выделяются наиболее активные участники, умеющие грамотно и доходчиво излагать свои мысли, а также способные убеждать и отстаивать свою точку зрения. При подборе новых членов, соответствующ-

щих идеологопропагандистской работе, вербовщиков в первую очередь интересует потенциальная способность кандидата воплощать экстремистские и террористические идеи.

Технологии вербовки в ряды МТО новых членов предельно просты и направлены, как правило, на людей, проводящих много времени в Интернете, находящихся в трудных жизненных ситуациях, одиноких, а также имеющих радикальные воззрения. При виртуальной работе вербовщики активно используют психолингвистические технологии «промывания мозгов» и внедрения в мировоззрение людей экстремистских ценностей, приукрашенных религиозной, националистической или иной «благообразной» риторикой. Такие приемы манипуляции сознанием людей в процессе интернет-переписки или онлайн-общения, когда отсутствует прямой контакт между собеседниками, формируют у большинства людей неосознанность действий большинства факторов, недопонимание ими собственного участия в экстремистской деятельности.

Для установления постоянных контактов с пользователями Интернета и поддержания с ними доверительных дружеских отношений вербовщиками выявляются личные проблемы людей и предлагаются варианты их решения посредством приобщения к «истинной вере» и совместной борьбы с «неверными» в рядах международных террористических организаций, уничтожения чиновников и работников силовых структур.

Наиболее активно пропаганда ведется в социальных сетях. Удобство такого подхода очевидно: соцсети позволяют террористам осуществлять вербовку, расположив к себе оппонента путем личной переписки, не требуют специальной подготовки и позволяют легко восстановить удаленный либо заблокированный ресурс.

Также местами вербовочной деятельности идеологов террористических организаций являются пенитенциарные учреждения системы ФСИН России.

Значительная часть спецконтингента данной категории – это не просто заключенные, имеющие устойчивое радикальное мировоззрение и обладающие навыками диверсионно-террористической деятельности, но и активно ведущие распространение экстремистской и террористической идеологии среди других категорий осужденных. Им удается вербовать новых сторонников, которые, освободившись из мест лишения свободы, начинают заниматься противоправной деятельностью, вливаясь в ряды бандподполья либо действуя автономно.

В целом анализ рассматриваемых причин и условий свидетельствует о том, что тезис о нормализации и стабилизации оперативной обстановки в СК ФО на основе статистических данных несколько преждевременный. Неблагополучная социальная реальность, подавление свобод в рамках межнациональных, этнических и религиозных конфликтах, создали благо-

приятные условия для усиления роли различных социальных групп, не редко преследующих экстремистские цели.

В 2017 году Северный Кавказ продолжает оставаться наиболее нестабильным регионом России, крайне болезненно реагирующим на малейшие внешние раздражители, что не всегда учитывается правоохранительными органами. Довольно высокий конфликтный потенциал СК ФО находит свое отражение в ниспадающем росте религиозного экстремизма среди молодежи и отсутствии доверия в некоторых субъектах округа к местным властям, которые не могут обеспечить приемлемый уровень их жизни, справиться с безработицей.

На этом фоне деятельность различных джихадистских структур, по-прежнему направлена на создание параллельной системы власти в северокавказских республиках. Лозунги «чистоты ислама» и освобождения территории от «неверных», оказывают серьезное влияние на новые поколения в знакомой, естественной и понятной для них среде сети «Интернет» и социальных сетях в частности.

Все это требует от Центров по противодействию экстремизму и всех государственных структур серьезных упреждающих мер, направленных на недопущение расширения экспансии экстремистских и террористических группировок на территории округа и распространения террористических угроз за пределы СК ФО.

Кислицын Николай Александрович,
преподаватель кафедры специальных дисциплин
Новороссийский филиал Краснодарского университета
МВД России

Тактика действий сотрудников оперативных подразделений в различных ситуациях оперативно-служебной деятельности

Рассмотрим примеры документирования преступлений и алгоритмы действий сотрудников уголовного розыска относящиеся к типовым оперативно-служебными ситуациями, возникающим в процессе профессиональной деятельности оперативных сотрудников. Вследствие многообразия ситуаций, встречающихся в деятельности оперативных подразделений, выделяются наиболее распространенные из них:

1. Работа в составе следственно-оперативной группы.

В ходе осуществления деятельности по выявлению и раскрытию преступлений, при рассмотрении заявлений или сообщений о преступлениях наиболее действенным и в то же время проблемным является взаимодействие подразделений ОВД путем:

- создания следственно-оперативных групп, старшими в которых исходя из подследственности, совершенного преступления бывают дознаватель или следователь;
- привлечения к деятельности следственной группы сотрудников оперативных подразделений, в том числе уголовного розыска;
- совместного анализа оперативно-служебных документов, отражающих результаты оперативно-розыскной деятельности, планирования, подготовки и проведения оперативно-розыскных мероприятий, следственных действий, а также оценки их результатов;
- сопровождения оперативными подразделениями расследования преступлений с момента возбуждения уголовного дела до вынесения по нему приговора суда.

При поступлении заявления о преступлении оперативный сотрудник в составе СОГ прибывает на место происшествия, где осмотр места происшествия должен сочетаться с оперативно розыскными мероприятиями, направленными на установление и задержание преступников по «горячим следам». В этих целях старший следственно-оперативной группы поручает оперативному сотруднику, участковым уполномоченным полиции и другим сотрудникам провести необходимый комплекс оперативно-розыскных мероприятий и других поисковых действий.

2. В ходе выполнения поручений следователя (дознавателя) сотруднику оперативного подразделения и другим участникам СОГ необходимо выполнить следующие действия:

- установить лиц, которые могли находиться вблизи от места происшествия (например, находились на остановке различного общественного транспорта, шли на работу или с работы);
- произвести опрос лиц, проживающих поблизости от места преступления
- отработать лиц, ранее судимых за совершение подобного рода преступлений или склонных к совершению конкретного вида преступления и проживающих на прилегающей территории совершения преступления;
- проверить места концентрации преступно-уголовно элемента (квартиры – притоны, подвалы, чердаки и др.);
- проверить общежития, расположенные в районе совершения преступления;
- отработать возможные пути подхода (отхода) лиц совершивших преступление к месту преступления, обнаружить возможные следы, оставленные на месте совершения преступления;
- провести совместно с лицами оказывающими содействие оперативным – сотрудникам, поквартирный опрос граждан проживающих вблизи места совершения преступления.
- установить автотранспорт и общественный транспорт, на которых злоумышленники могли скрыться с места совершения преступления.

Основная деятельность по установлению места нахождения и розыску преступников по совершенному преступлению, в основном, лежит на оперативных сотрудника. Согласно федеральным законам «О полиции», «Об оперативно-розыскной деятельности» и другим действующим нормативным правовым актам МВД России сотрудник уголовного розыска осуществляет необходимые оперативно-розыскные мероприятия по установлению, обнаружению и задержанию лиц, подозреваемых в совершении преступления, доставляет их в органы внутренних дел для осуществления процессуальных действий.

Сотруднику уголовного розыска необходимо помнить о соблюдении требований оперативно-розыскного и уголовно-процессуального законодательства Российской Федерации при проведении оперативно-розыскных мероприятий, проведении осмотра и обыска в жилище, что имеет определенные ограничения при их проведении.

Взаимодействие сотрудников органов внутренних дел важно не только на первоначальном этапе, но и на последующих этапах расследования преступления, данное взаимодействие заключается в эффективном оперативном сопровождении со стороны сотрудников оперативных подразделений согласованных действиях всех подразделений и служб, направленных на раскрытие и расследование совершенного преступления.

Из объема первоначально полученной информации сотрудники оперативных подразделений совместно со следователем (дознавателем) выдвигает версии совершенного преступления, требующие проверки и подтверждения в ходе дальнейшего расследования уголовного дела.

Сотруднику оперативного подразделения необходимо помнить, что его организационно-тактические действия на месте происшествия и первоначальные оперативно-розыскные мероприятия зависят от видов совершенных преступлений и различны по своему содержанию.

3. При обнаружении или получении сообщения об обнаружении взрывчатых веществ и взрывных устройств, вероятных взрывоопасных предметов (веществ), а также об угрозе взрыва.

В данном случае сотрудники уголовного розыска обязаны:

- незамедлительно сообщить об этом оперативному дежурному по УМВД (ОМВД);

- не производить каких-либо самостоятельных действий с обнаруженным предметом (веществом): подходить близко к ВВ, ВУ, брать в руки и перемещать их вблизи с металлическими предметами;

- находясь рядом с обнаруженным предметом (веществом), выключить все радиоуправляемые устройств; (сотовые телефоны, пейджеры, радиостанции, компьютеры и т.д.);

- принять меры к удалению из опасной зоны населения, взяв данную зону под охрану до прибытия специалистов по обезвреживанию и распознаванию ВВ, ВУ;

- принять меры к прекращению движения транспортных средств на прилегающей территории, обеспечив объездные пути и оказывая содействие беспрепятственному проезду автомобилей оперативных и аварийно-спасательных служб;

- принять меры для задержания лиц, имеющих причастность к ВВ, ВУ;

- осуществлять мероприятия по восстановлению и поддержанию общественного порядка;

- фиксировать и устанавливать личность лиц, производящих фото-, видеосъемку на месте происшествия;

- по прибытии на место происшествия дежурной СОГ доложить об известных обстоятельствах происшествия, предпринятых мерах и в дальнейшем действовать по указанию руководителя СОГ.

4. Действия сотрудника уголовного розыска после взрыва.

В этом случае сотрудник уголовного розыска должен:

- сообщить дежурному по УМВД (ОМВД) о масштабах и последствиях взрыва;

- эвакуировать в безопасную зону людей, находящихся вблизи места взрыва;

- до прибытия скорой медицинской помощи оказать первую медицинскую помощь пострадавшим и при необходимости организовать доставку в медицинские учреждения;

- обеспечить охрану и ограждение места взрыва, не позволять никому, кроме работников скорой помощи и аварийных служб, приближаться к месту взрыва или уносить оттуда какие-либо предметы;

- ограничить или запретить движение автотранспортных средств на прилегающей территории;

- принять меры к установлению очевидцев взрыва и для задержания подозреваемых;

- осуществлять мероприятия по поддержанию общественного порядка.

Следует иметь в виду, что ВВ, ВУ могут быть оформлены как промышленные товары (мыло, стиральный порошок и др.), замаскированы под продукты питания, перевозимые в различной таре (ящики, бидоны, мешки и др. упаковки), автомобильные принадлежности: (канистры, огнетушители и т.д.).

5. По предупреждению возможных террористических актов.

Общие профилактические мероприятия включают в себя сбор информации о подготовке террористических актов и организацию работы по выявлению и предупреждению таких актов.

Источниками информации о подготовке террористических актов могут быть:

- сведения, полученные из опросов водителей транспортных средств, особенно следующих из Северо-Кавказского региона Российской Федерации;

- сведения, полученные из опроса лиц, прибывающих в Российскую Федерацию для трудовой деятельности из ближнего зарубежья;
- ориентировки оперативных подразделений ОВД;
- информация, поступающая от граждан, должностных лиц через средства массовой информации;
- личные наблюдения в процессе несения службы с учетом складывающейся ситуации и др.

При получении подобной информации, независимо от ее источника, необходимо:

- немедленно доложить оперативному дежурному по УМВД (ОМВД);
- принять меры по выявлению лиц, имеющих отношение к данной информации;
- установить и записать все необходимые установочные данные о заявителях, подозреваемых, лицах, и другую информацию, имеющую значение для выяснения обстоятельств.

Организация работы по выявлению и предупреждению возможных террористических актов осуществляется в тесном взаимодействии сотрудников уголовного розыска с сотрудниками иных подразделений и служб ОВД, ДПС (на маршрутах патрулирования и стационарных постах); ППС (на маршрутах патрулирования) с целью сбора информации и проведения комплекса согласованных действий и поисковых мероприятий.

Таким образом, правильно выбрана тактика действий сотрудников оперативных подразделений обеспечивает своевременное установление, задержание лиц совершивших преступления. Обеспечивает своевременную, правильную и безотлагательную помощь лицам, ставшим жертвами различного вида преступлений.

Красников Вадим Николаевич,
старший преподаватель кафедры оперативно-разыскной деятельности
и специальной техники Ставропольского филиала
Краснодарского университета МВД России

Правовые основы взаимодействия оперативных подразделений органов внутренних дел с общественностью

Для успешного функционирования современного российского общества как полноценной структуры очевидно необходимо его плотное взаимодействие с государством в целом и государственными органами в частности при решении наиболее сложных политических и социально-экономических вопросов. Вместе с тем, обеспечение системного взаимодействия между органами власти и институтами гражданского общества, основной целью которого является защита конституционных прав и свобод

человека, рассматривается в качестве важнейшего требования не только существования демократического общества, но и управления в нём.

В том случае, когда такое взаимодействие становится нестабильным, не укрепляется путём постоянных плодотворных контактов с целью решения общих, актуальных для обеих сторон задач, постепенно разрушается взаимосвязь в не без того сложно складывающихся отношениях между обществом и правоохранительной системой, а в частности и полицией, что в значительной мере усложняет соблюдение одного из важнейших принципов стабильности государства – безопасности его граждан, их уверенности в постоянной защите с его стороны.

Данные обстоятельства стали ключевым моментом в возникновении правовых и организационных форм обеспечения общественного порядка.

В Российском государстве это стало актуализироваться начиная с XVI-XVII вв. Как раз в это время государство осознало необходимость осуществления функции по охране общественного порядка и создало актуальные для того времени формы участия граждан в этой области общественной жизни.

В наши дни, особенно после принятия Федерального Закона «О полиции», вопросы взаимодействия государства и общества в осуществлении функции по пресечению и раскрытию правонарушений заметно актуализировались.

Ежегодно на расширенном заседании коллегии МВД России вопросам взаимодействия полиции с представителями тех или иных общественных объединений отводится немаловажная роль.

Так, 28 февраля 2018 года президент Российской Федерации В.В. Путин в своём выступлении сказал, что одной из основных задач, стоящих перед органами внутренних дел, является обеспечение безопасности в общественных местах. Необходимо оперативное реагирование на любые нарушения порядка на улицах, транспорте, на спортивных, зрелищных мероприятиях, широкое применение при этом современных технических средств, привлечение для помощи дежурных нарядов дружинников, других общественных структур.¹

В свою очередь, министр внутренних дел В.А. Колокольцев отметил, что в прошедшем году сотрудники полиции выполнили значительный объём розыскной работы. Ими было задержано 61 тысяча лиц, скрывавшихся от органов дознания, следствия и суда, установлено местонахождение свыше 40 тысяч без вести пропавших. Поисково-спасательные операции, в том числе по розыску детей, осуществлялись совместно с подразделением МЧС России и представителями волонтерского движения. В этой связи он упомянул, что органы внутренних дел заинтересованы в дальнейшем раз-

¹ Выступление Президента Российской Федерации В.В. Путина на расширенном заседании коллегии МВД России (28 февраля 2018 года). URL: <http://www.kremlin.ru/events/president/news/56949>.

витии диалога с добровольческими организациями и будут оказывать им всемерное содействие.

Но главным и самым объективным критерием оценки для органов внутренних дел является мнение граждан. По данным независимых исследовательских центров, наблюдается устойчивая тенденция роста доверия к сотрудникам полиции.¹

Вместе с тем, любая деятельность, осуществляемая на территории нашего государства должна осуществляться в соответствии с Конституцией Российской Федерации и соответствующими нормативными правовыми актами.

Вопросы, касающиеся возможности создания общественных объединений нашли своё отражение в статье 30 Конституции, а в статье 32 сказано, что граждане Российской Федерации имеют право участвовать в управлении делами государства как непосредственно, так и через своих представителей.²

То есть, осуществлять функцию взаимодействия с органами государственной власти, в том числе и в вопросах борьбы с преступлениями и правонарушениями, человек может как самостоятельно, так и в составе общественных объединений правоохранительной направленности.

С появлением Федерального закона «О полиции» одним из основных принципов деятельности современной полицейской структуры стало выступать общественное доверие и поддержка граждан. Отсюда возникла острая необходимость разрабатывать всё новые и новые механизмы взаимодействия полиции с обществом, причём эти механизмы должны обобщить в себе положительную практику как отечественных форм взаимодействия прошлых лет, так и иностранного опыта.

В Федеральном законе «О полиции» отражены правовые основы взаимодействия органов внутренних дел, в том числе и их оперативных подразделений с общественными объединениями. Ключевые моменты организации взаимодействия и сотрудничества полиции с обществом отражены во 2, 3 и 10 главах указанного закона.

Согласно статьи десятой настоящего Федерального закона, определяющей основные аспекты такого взаимодействия и сотрудничества, полиция при осуществлении своей деятельности взаимодействует с общественными объединениями, организациями и гражданами, может использовать возможности общественных объединений и организаций, оказывает содействие общественным объединениям и организациям.

¹ Выступление министра внутренних дел Российской Федерации В.А. Колокольцева на расширенном заседании коллегии МВД России (28 февраля 2018 года). URL: <http://www.kremlin.ru/events/president/news/56949>.

² Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (в действующей редакции) // Собрание Законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.

Применительно к оперативным подразделениям органов внутренних дел, нельзя не отметить положения, нашедшие отражение в статье 13 этого же нормативного правового акта. Так, согласно пункта 34, полиции для выполнения возложенных на нее обязанностей предоставляется право привлекать граждан с их согласия к внештатному сотрудничеству; устанавливать негласное сотрудничество с гражданами, изъявившими желание конфиденциально оказывать содействие полиции на безвозмездной или возмездной основе; объявлять о назначении вознаграждения за помощь в раскрытии преступлений и задержании лиц, их совершивших, и выплачивать его гражданам; поощрять граждан, оказавших помощь полиции в выполнении иных возложенных на нее обязанностей; привлекать для консультаций в установленном порядке специалистов государственных и муниципальных органов, организаций с сохранением за ними заработной платы (денежного содержания) по основному месту работы (службы).¹

Что касается денежного вознаграждения за помощь в раскрытии преступлений гражданам, оказывающим конфиденциальное содействие, то, как справедливо отмечает в своих трудах Н.П. Голяндин, законодатель необоснованно ограничил меры стимулирования для лиц, оказывающих конфиденциальное содействие в борьбе с преступностью. Автором предлагается целый комплекс мер по повышению заинтересованности конфиденентов в конечном результате своей деятельности. Это и повышение уровня денежных выплат за результативное содействие, и рассмотрение вопроса о досрочном освобождении или смягчении наказания, и предоставление возможности получения конфидентами государственных наград, и, наконец, урегулирование вопросов, связанных с пенсионным обеспечением лиц, оказывающих конфиденциальное содействие оперативным подразделениям органов внутренних дел.²

Вопросы взаимодействия общественности с правоохранительными органами в решении задач по охране правопорядка в нашей стране возникли не в советский период, а гораздо раньше, – во времена царской России. К примеру добровольные народные дружины, возникли в Москве в далёком 1881 году. Взаимодействие с общественными формированиями правоохранительной направленности показало, что добровольные народные дружины и другие гражданские объединения могут оказывать серьёзный вклад в обеспечение порядка в обществе. Федеральный закон от 2 апреля 2014 года №44-ФЗ «Об участии граждан в охране общественного порядка» закрепил право граждан оказывать необходимую помощь правоохранительным органам в вопросах поддержания правопорядка в стране.

¹ Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // Собрание Законодательства Российской Федерации. – 2011. – № 7. – Ст. 900.

² Голяндин Н.П. Проблемы обеспечения оперативно-розыскной деятельности: проблемы и решения: доклад / Н.П. Голяндин. - Краснодар: КрУ МВД России, 2016. С.41.

Исходя из положений данного нормативного акта граждане – участники общественных формирований информируют органы внутренних дел о правонарушениях и угрозах общественному порядку, принимают участие в поиске лиц, пропавших без вести, привлекаются к внештатному сотрудничеству с полицией, а также могут создавать добровольные, в том числе и казачьи, дружины.¹

Немаловажную роль в нормативном регулировании вопросов взаимодействия оперативных подразделений органов внутренних дел с общественностью играет Федеральный закон «Об оперативно-розыскной деятельности».

Так, в статье шестой говорится о том, что должностные лица органов, осуществляющих оперативно-розыскную деятельность, решают её задачи при помощи лиц, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе. Статья пятнадцатая определяет органам, осуществляющим оперативно-розыскную деятельность, право на установление отношений сотрудничества на возмездной или безвозмездной основе с лицами, желающими оказывать содействия оперативным подразделениям. В семнадцатой статье обозначено, что человек, изъявив своё согласие, может привлекаться оперативными подразделениями для подготовки и проведения оперативно-розыскных мероприятий, сохраняя конфиденциальность своего участия, но он, в свою очередь, должен хранить в тайне информацию, ставшую ему известной в процессе осуществления данной деятельности.

Здесь же перечислены условия осуществления такого взаимодействия, а так же запреты, связанные с невозможностью привлечения к конфиденциальному содействию на контрактной основе отдельных категорий граждан.²

Помимо Федерального закона «Об оперативно-розыскной деятельности», вопросы использования содействия граждан оперативными подразделениями нашли отражение в ведомственных нормативных правовых актах закрытого характера, но даже в них не учтены в полной мере все категории лиц, оказывающих содействие, не определён их правовой статус и методика взаимодействия с правоохранительными органами.

Таким образом, вопросам взаимодействия правоохранительных органов, а в частности и оперативных подразделений органов внутренних дел с общественностью в целях поддержания правопорядка и борьбы с

¹ Федеральный закон от 02.04.2014 №44-ФЗ «Об участии граждан в охране общественного порядка» // Собрание Законодательства Российской Федерации. - 2014. - №14. - Ст. 1536.

² Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание Законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

преступностью в настоящее время отводится немаловажная роль. В рамках написания статьи нами освещены только отдельные аспекты правоотношений в этой сфере. Но даже при таком рассмотрении очевидно, что многие вопросы, касающиеся этой области правоохранительной деятельности, не учтены в полной мере в нормативных актах её регламентирующих, и по мнению автора, требуют скорейшего разрешения.

Молько Максим Евгеньевич,
курсант Краснодарского университета МВД России;
Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-разыскной деятельности в ОВД
кандидат юридических наук

Некоторые особенности выявления наркотических закладок

Наркотические закладки используются для скрытой передаче наркотических веществ от поставщика к покупателю. Они чаще всего представляют с собой небольшой пакет, который закладывается в общественных местах (почтовый ящик, стена жилого здания, и т. д.). Существует определенная схема распространения наркотических веществ: потребитель оформляет заказ через Интернет, затем дилер или курьер прячет закладку в определенном месте, затем сообщает координаты покупателю. Сами организаторы наркотрафиков не занимаются распространением закладок, курьеры напрямую не передают наркотические вещества с целью сбыта, а через подставных лиц передают часть товара. Данных подставных лиц находят через сеть Интернет, которые хотят легкой наживы. Сложностью данного вида сбыта наркотических веществ является процесс поиска лиц, которые являются наркодельцами усложняется, так как они особо ни с кем не взаимодействуют из сбытчиков, следовательно привлечь данных лиц к ответственности очень затруднительно.

Как правило, закладки наркотических веществ используют ничем не примечательные и малолюдные места – подъезды, заброшенные стройки, подвальные помещения, деревья, кустарники, почтовые ящики. Покупатели наркотических веществ через различного рода платежных систем (WebMoney, Яндекс.Деньги, Qiwi-кошелек, а также перечисление денежных средств через платежные банковские системы, такие как Сбербанк онлайн).

Как уже было указано выше, лица, занимаются распространением наркотических средств не работают в одиночку. Существует определенная иерархия лиц, которые занимаются передачей наркотиков от наркодельца к покупателю:

1. Организационно-управленческий уровень. Эти лица, которые являются организаторами по осуществлению поставок наркотических

средств и их передача другим сообщникам для последующего его расфасовывания.

2. Организационно-обеспечивающий уровень. Данный уровень включает в себя: «диспетчеров», «массажистов». «Диспетчеры» занимаются сбором и хранением информации о местах расположения так называемых тайников. «Массажистами» являются лица, которые занимаются отысканием помещений, приборов, технических и иного оборудования для удобного приготовления, расфасовки и хранения наркотических средств.

3. Исполнительный уровень. В него входят так называемые «бегунки» – это лица, которые непосредственно доставляющие расфасованные ранее свертки с наркотическими средствами в тайники. Данная преступная деятельность регламентируется статьей 228 Уголовного кодекса Российской Федерации за незаконное приобретение, хранение, перевозку, изготовление, переработку наркотических средств без цели сбыта установлено наказание. Данная статья предусматривает наказание для лиц, которые непосредственно покупают наркотические средства. Такому лицу грозит следующие виды наказания: штраф в размере до 500 тысяч рублей или в размере зарплаты или иного дохода осужденного за период до трех лет либо ограничение или лишение свободы на срок до 15 лет.

Для лиц, которые непосредственно осуществляют закладки с целью сбыта, Уголовным кодексом установлена еще более строгая ответственность. Статья 228.1, которая предусматривает наказания для лиц, занимающихся незаконным производством, сбытом или пересылкой наркотических средств, психотропных веществ или их аналогов. Данная категория лиц может лишиться свободы сроком до 20 лет и со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет без такового или пожизненным лишением свободы. С широким распространением средств компьютерной техники и сети интернет создает расширенные возможности для сбыта наркотических веществ. Как правило сбытчики наркотических средств напрямую не распространяют информацию о том, что именно здесь можно приобрести наркотические средства, а под видом различных сайтов по оказанию услуг и распространения товаров производят сбыт различных наркотических средств. Инструментом контроля и мониторинга сети интернет на предмет продажи наркотических средств является Роскомнадзор. Большая часть сайтов, занимающихся продажей наркотических веществ регистрируется на зарубежных доменах, что не позволяет пресекать работу данных сайтов, а также привлекать разработчиков и сбытчиков к ответственности. Особую опасность представляют специализированные форумы в различных социальных сетях. На них происходит обсуждение лекарственных средств, которые дают одурманивающий эффект. Самым крупным интернет-форумом, который регистрирует заявки на покупку данных препаратов без рецептов является сайт Legal.RC, доступ к которому в Рос-

сийской Федерации запрещен. Однако существует разновидность программ, позволяющих свободно посещать данные форумы, даже если они запрещены в Российской Федерации. Одним из таких ярких примеров программ является TOR.

TOR – это свободное и открытое программное обеспечение. Это вид системы которая позволяет устанавливать анонимную информацию о весе, цене предлагаемого наркотика, а также способах связи и оплаты размещается на сайте сети Интернет. Передача данных наркотических средств происходит непосредственно при помощи закладок. «Диспетчер», представляет подробные координаты место нахождения данной закладки, а также указывает промежутки времени в течении которых данная закладка будет находится на месте. В последующем, покупатель через платежные системы производит оплату. Еще одним способом общения «диспетчера» с покупателем возможно осуществлять при помощи таких социальных сетей как: «WhatsApp, «Viber», «Skype», «ISQ» и других. В этих и других социальных сетях происходит общение не только с покупателями наркотических средств, но и общение между различными уровнями преступной среде, занимающиеся сбытом наркотических средств. Через данные социальные сети происходит передача информации о новых местах, где можно класть закладки, система платы за каждую удачную сделку с покупателем, система штрафов, в случае, если закладка не дошла до конечного потребителя, а также подробная инструкция о том, как незаметно для окружающих перевозить и класть свертки с наркотическими веществами в указанные места.

Методика поиска лиц, занимающихся бесконтактным сбытом наркотических веществ.

Учитывая специфику указанного преступления, методика расследования будет заключаться в проведении следующих оперативно-розыскных мероприятий и следственных действиях:

1) Наблюдение за лицами, которые подозреваются в подготовке, совершении и сокрытии преступления.

2) Привлечение конфиденентов, которые способны обеспечивать правоохранительные органы необходимой информацией.

3) Прослушивание телефонных переговоров подозреваемых.

4) Получение компьютерной информации, при мониторинге интернет-страниц, в которых содержаться скрытая реклама наркотических средств.

5) Опрос граждан, которые живут с подозреваемым в одном доме, дворе, районе.

6) Проведение проверочной закупки, под видом покупателя договорится с лицом, который непосредственно производит закладки (бегунком).

Сотрудник оперативного подразделения при помощи ряда действий может не только найти закладку, но и найти всех лиц, причастных к совершению данного вида преступления. На первоначальном этапе, необхо-

димо сделать акцент на тех лиц, которые уже привлекались к уголовной ответственности. Целесообразней всего привлекать в качестве информаторов лиц, которые уже привлекались за употребления наркотических средств, а также лиц, которые стоят на учете в наркологическом учете. Данные лица в больше части уведомлены, в каких местах закладываются наркотические средства и в какой промежуток времени чаще всего производится закладка наркотических средств. Далее необходимо найти контакт с так называемыми «Диспетчерами», чтобы произвести проверочную закупку данных наркотических веществ. Договорившись о месте и времени, где непосредственно будет лежать наркотическое вещество произвести наблюдение, за данным местом. Так как бегунок, может заложить наркотическое вещество за долго до того, как будет договоренность о месте встречи с покупателем, то необходимо непрерывно производить наблюдение в течение 3-4 дней. Наблюдение необходимо вести с помощью видео и аудио фиксирующих средств, иначе причастность данного лица к попытке бесконтактного сбыта наркотических веществ будет не доказана. Необходимо зафиксировать момент того, что данное лицо закладывает сверток с наркотическим веществом в определенное место. Затем необходимо произвести наблюдение за данным лицом, возможно, что он приведет к другим местам, где производятся закладки наркотических веществ. Произвести задержания данного лица. Изъять у данного лица средства связи. Далее необходимо получить у операторов сотовой связи детализацию входящих и исходящих звонков абонентских номеров, принадлежащих лицам, занимающимися бесконтактному сбыту наркотических веществ. Получить у операторов сотовой связи, которыми пользовался кто-то из членом преступной организации, ознакомится с содержанием входящих и исходящих смс сообщений, а также произвести распечатку диалогов, если это представляется возможным, через социальные сети. После получения разрешения у суда, необходимо произвести обыск помещения, где непосредственно живет лицо, попытавшееся сбыть наркотическое вещество. При проведении обыска следует уделить особое внимания не только на привычную компьютерную технику, но и иметь в виду, что существует телевизоры нового поколения – «Smart TV», так как через них можно также выходить через Интернет. Также произвести обследования социальных сетей, находящихся как в телефоне, так и в компьютере, в том числе и в телевизорах нового поколения. Также необходимо истребовать у банковских сотрудников распечатки о состоянии на лицевых счетах, а также лиц, от которых были переводы на лицевой счет задержанного. После получения необходимой информации у задержанного лица, возможно найти и других лиц, которые занимаются сбытом наркотических средств, также найти каналы поставки наркотиков, места, где расфасовываются различного рода наркотических веществ.

Если наркотики менять на мобильный телефон, любую другую вещь, получать электронные деньги за наркотики на Webmoney, QIWI, обычную карту банка, производить продажу путем «закладки» в тайном месте, все это будет являться сбытом наркотиков и квалифицироваться по части 4 ст. 228 УК РФ. Одним из немаловажных моментов данной статьи является конфискация имущества и огромный штраф, а также помним о том, что в тюрьме сбытчиков не любят и не уважают, так как своими деяниями они посадили не одного человека на иглу, разрушили семьи, принесли неизлечимые болезни.

В заключении необходимо отметить, что в доказывании факта сбыта наркотиков, присутствует огромное количество нюансов, такие как «свои понятия», неправильное составление документов, нарушение конституционных прав. Грамотный защитник, обязательно найдет их, и дело как говорят – развалится. Поэтому оформлять оперативно-служебные документы необходимо в соответствии с законом и ведомственными нормативными актами.

Петухов Андрей Юрьевич,
старший преподаватель кафедры
оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат педагогических наук

Современные информационные технологии и преступность в сфере незаконного оборота наркотиков

Интернет, платежные системы, мессенджеры, интернет магазины, сегодня это неотъемлемая часть современного общества. В тоже время, несмотря на вполне очевидные плюсы этих средств телекоммуникации, использование их в преступной деятельности вынуждает государство внимательно следить за этим полем правоотношений и своевременно регулировать их.

Если рассматривать преступления связанные с незаконным оборотом наркотиков, то мы можем констатировать значительное увеличение количества таких преступлений совершаемых с использованием средств сети Интернет, электронных платёжных систем и т.п. Объемы данного рынка стабильно увеличиваются, приобретая все более новые и современные очертания. И эта тенденция очевидна ввиду активного использования средств современных телекоммуникаций современной молодежью.

Развитие информационных технологий, широкое использование их в повседневной деятельности гражданами страны, позволило преступным группировкам не только взять на вооружение достижения современной техники и телекоммуникационных систем, но и изменить сам характер

преступной деятельности, позволило формировать транснациональные организации и преступные сообщества на более высоком технологическом уровне, меняя сам характер преступной деятельности. Следует заметить, что это достигается не только на федеральном и межрегиональных уровнях, но и на международном уровне. И здесь особенно актуальной проблемой является бесконтактный сбыт наркотиков осуществляемый посредством сети Интернет, интернет-магазинов, мессенджеров, и при активном использовании электронных платежных средств.

В целях повышения эффективности борьбы с такими формами незаконного оборота наркотиков, в 2010 году в России принята Стратегия государственной антинаркотической политики Российской Федерации до 2020 года. Разработка данного нормативного акта была обусловлена, прежде всего, активизацией деятельности транснациональной преступности, усилением терроризма, экстремизма, появлением новых видов наркотических средств и психотропных веществ (далее – наркотики), усилением негативных тенденций, таких как устойчивое сокращение численности населения России, в том числе уменьшение численности молодого трудоспособного населения вследствие расширения масштабов незаконного распространения наркотиков.¹

В тоже время, стратегией национальной безопасности Российской Федерации до 2020 года, утвержденной Президентом Российской Федерации 12 мая 2009 г., одним из главных источников угроз национальной безопасности признана деятельность транснациональных преступных группировок и организаций, связанная с незаконным оборотом наркотиков и их прекурсоров.²

Несмотря на это, в период с 2009 года по 2017 год сколько-нибудь значительного перелома в сфере борьбы с незаконным оборотом наркотиков на территории нашей страны не произошло. Это подтверждает принятое решение Президента страны о ликвидации Федеральной службы по контролю за оборотом наркотиков ввиду ее неэффективности.

В рассматриваемый период государство не раз предпринимало попытки оптимизировать законодательство в рассматриваемом поле правоотношений, вводя все новые санкции в рамках уголовного законодательства. Неоднократно менялись подходы в оценке действий лиц участников незаконного оборота наркотиков, в частности декриминализация деяний

¹ Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2020 года. [Электронный ресурс]: указ президента № 690 : [принят 09.06.2010] // СПС «КонсультантПлюс». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_101259/ (дата обращения: 01.11.2017).

² О Стратегии национальной безопасности Российской Федерации до 2020 года. [Электронный ресурс] : указ президента № 537 : [принят 12.05.2009] // СПС «КонсультантПлюс». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_87685/ (дата обращения: 01.11.2017).

связанных с хранением наркотических средств без цели сбыта, с целью на законодательном уровне вычленив лиц больных наркоманией и лиц непосредственно участвующих в незаконном сбыте.

Наряду со значительными изменениями в уголовном законодательстве введенными в 2012 году, в этот же период уточняются размеры наркотических средств для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса, что позволяет дифференцировать наказания в зависимости от количества наркотических средств, вводится понятие аналог наркотического средства, определяется порядок признания аналогового вещества наркотическим.¹

Увеличивается давление на Интернет, путем организации блокировок сайтов с противоправным контентом посредством службы Роскомнадзора, реализуется политика подрыва экономических основ наркобизнеса посредством вовлечения службы по финансовому мониторингу. Следует отметить, что все вышеуказанные меры не возымели ожидаемого эффекта, уровень владения современными телекоммуникационными системами, реакция на изменения законодательства у преступных группировок оказались значительно выше, чем реакции законодательных инициатив со стороны государства. Хотя, справедливости ради, нужно отметить, что функция разграничения наказания, вычленение больных наркоманией из спектра ответственности за хранение наркотиков без цели сбыта все же стало эффективной мерой. Реализация мер борьбы с аналогами наркотических веществ, веществ, не внесенных в соответствующие списки, так же позволило эффективно бороться с новыми наркотиками.

И все же, основными проблемами остаются проблемы процессуальные и сложности документирования преступлений совершаемых посредством сети Интернет. Прежде всего, это высокая латентность совершаемых преступлений, обусловленная высокой степенью применения различных анонимайзеров преступными группами, при этом реализуется главный принцип отсутствие физического контакта между членами преступных группировок, что значительно затрудняет как процесс документирования, так и процесс последующего доказывания по уголовным делам такой категории, так как субъекта преступления установить очень сложно, а в ряде случаев просто невозможно.

Еще одним не маловажным фактором является осуществление механизма сбыта посредством тайниковых закладок с наркотическими сред-

¹ Об утверждении значительного, крупного и особо крупного размеров наркотических средств и психотропных веществ, а также значительного, крупного и особо крупного размеров для растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса Российской Федерации»

ствами. Этот метод сбыта остается преимущественным уже на протяжении более 7 лет. И эффективных мер борьбы с ним не найдено и по сей день.

Еще более важным негативным фактором в ходе документирования и последующего расследования уголовных дел, связанных с реализацией наркотиков посредством сети Интернет с использованием бесконтактного сбыта наркотиков, является широкое, а лучше сказать, преимущественное использование электронных платежных средств. На первоначальном этапе преступники использовали преимущественно QIWI Кошельки. С учетом того, что такой электронный кошелек является платежной системой, которая позволяет осуществить платежи за услуги и денежные переводы с мобильного телефона, работающего в стандарте GSM, сбытчик наркотиков имеет возможность получить денежные средства находясь на любой территории. Впоследствии используя счета открытые на подставных лиц в различных коммерческих банках осуществлялись транзакции с целью вывода денежных средств с территории Российской Федерации.

Сегодня же, в преступной деятельности активно используются различные криптовалюты. Данный рынок вообще тяжело контролируем. А, следовательно, использование этих средств в целях осуществления расчетов между покупателями и продавцами наркотиков постоянно растет. На текущий момент в мире зарегистрировано более 1000 различных видов криптовалют и их число постоянно растет.

В тоже время, несмотря на выше обозначенные проблемы, следует отметить, что государство с 2016 года взяло курс, рассчитанный на применение системных мер контроля информационной среды. Основными нормативно-правовыми актами, которые претерпели значительные изменения в этой сфере, являются:

1. Федеральный закон «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» от 06.07.2016 N 374-ФЗ.

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 29.07.2017) «О персональных данных».

3. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон «О внесении изменений в статью 5 Федерального закона О защите детей от информации, причиняющей вред их здоровью и развитию и отдельные законодательные акты Российской Федерации в целях защиты детей от информации, пропагандирующей отрицание традиционных семейных ценностей» от 29.06.2013 N 135-ФЗ (последняя редакция).

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации».

Так же следует выделить ряд мер направленных на осуществление контроля за работой различных мессенджеров и т.п. С ноября 2016 года Федеральная служба безопасности Российской Федерации получила техническую возможность перехвата информации, отправляемой пользователями таких популярных мессенджеров, как WhatsApp и Viber. Теперь на базе их дата-центров появились сервера, подключенные к системе СОРМ (система технических средств для обеспечения функций оперативно-разыскных мероприятий).

Очевидно, что такие шаги это требования времени, так как только комплексные меры, в конечном счете, позволяет взять под контроль имеющиеся технические ресурсы сети, по крайней мере, зарегистрированные на территории Российской Федерации. Что в какой-то степени позволит эффективно бороться с региональными, межрегиональными преступными наркогруппировками на территории России.

Пестрецов Михаил Алексеевич,
преподаватель кафедры оперативно-разыскной деятельности
и специальной техники Крымского филиала
Краснодарского университета МВД России,
кандидат юридических наук

Особенности получения оперативно-розыскной информации в сети Интернет

Общепризнано, что принципами оперативно-розыскной деятельности являются законность, конспирация, сочетание гласных и негласных методов и средств, используемых в оперативно-розыскной деятельности. Данные положения закреплены в Федеральном законе «Об оперативно-розыскной деятельности».¹ Эти принципы имеют прямое отношение для получения информации в сети Интернет.

На просторах сетевого пространства можно получить оперативную информацию о противоправной деятельности отдельных лиц, а также ссылки на сетевые сайты и адреса, которые могут содержать запрещенные к распространению материалы. Одним из эффективных способов получения информации является оперативный поиск, с его помощью можно не только установить конкретных лиц причастных к совершению преступлений, но и подобрать лицо согласное для конфиденциального сотрудничества. В процессе получения оперативно-значимой информации в сети Интернет возможно проведение такого оперативно-розыскного мероприятия

¹ Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ.

как «опрос», который можно проводить в отношении граждан в электронном виде, что не противоречит действующему законодательству.

Одним из приемов оперативного поиска является оперативно-розыскной мониторинг.

Процесс оперативно-розыскного мониторинга состоит из сменяющих друг друга фаз, а именно:

- сбор общей информации о среде функционирования;
- выявление информации о криминологической обстановке и объекте оперативного внимания на просторах сетевого пространства;
- поиск первичной оперативно-розыскной информации о конкретных преступлениях; сбор и оценка информации о силах и средствах правоохранительных органов;
- анализ результативности противодействия преступности; прогнозирование ее развития и тенденций.

Одной из главных задач «мониторинга» является получение и анализ о лицах и объектах, представляющих оперативный интерес. Для решения задач оперативные сотрудники используют различные поисковые системы, в которых можно получить информацию по заданным параметрам.

Установить первоначальные данные о лицах представляющие оперативный интерес можно получить на открытых социальных сайтах (Одноклассники, Facebook, ВКонтакте). В ходе проделанной работы оперативные сотрудники могут выявить информацию криминального характера, а именно: веб-сайты пропагандирующие насилие, педофилию, порнографию и др.

Также оперативные сотрудники в ходе общения в сети Интернет, могут выявить граждан, которых можно будет привлекать для конфиденциального сотрудничества. Данные граждане в последующем будут привлекаться для решения определенных задач возникающие в сетевом пространстве, для получения оперативно-розыскной информации. При налаживании доверительных контактов с гражданином, оперативный сотрудник получает информацию о сайтах и лицах криминальной активности, а также о способах и методах совершения преступлений. Возникает новое понятие в оперативно-розыскной деятельности как сетевой конфидент, лицо привлекаемое к выполнению узконаправленных задач в сети Интернет.

Необходимо отметить, что все тактические приемы, в зависимости от оперативно-розыскной ситуации, по характеру решаемых задач могут быть направлены на обеспечение оперативной разработки и шифрование источников получения негласной информации; негласное выявление и хранение фактических данных, которые могут быть использованы в качестве доказательств в уголовном производстве; осуществление оперативно-профилактического воздействия на лиц, склонных к совершению преступления; решение конфликтных ситуаций, нейтрализацию противодействия со стороны разрабатываемых лиц; создание условий, необходимых для

проведения ОРМ; создание условий, гарантирующих результативность оперативно-тактических мероприятий; обеспечение негласности мероприятий, хранение в процессуальном изъятии предметов и документов, которые могут быть доказательствами преступной деятельности; другие тактические меры воздействия на оперативно-тактическую ситуацию с целью ее изменения на более благоприятную и т. д.¹

В настоящее время в оперативно-розыскной работе накопился значительный практический материал, который требует всестороннего теоретического осмысления, разработки на его основе и внедрения в практику новых тактических приемов. С совершенствованием законодательной базы по борьбе с преступностью, новыми научно-техническими разработками и внедрением в практику работы органов внутренних дел современных средств специальная техника научных разработок тактических приемов оперативно-розыскной работы рассматривается как одна из актуальных задач. В настоящее время, по нашему мнению, нет единого подхода по многим вопросам теории оперативно-розыскной деятельности, в том числе и по вопросам оперативно-розыскной тактики.

Тактика оперативно-розыскной деятельности гораздо шире, чем система «научных подходов». Тактика включает элементы планирования, вопросы использования данных других наук – логики, педагогики, психологии и оперативно-розыскной психологии. Получение оперативно-розыскной информации в сети Интернет, имеет свои особенности, которые применяются в конкретной ситуации оперативным сотрудником.

Сафронов Андрей Алексеевич,

доцент кафедры оперативно-розыскной деятельности в ОВД

Краснодарского университета МВД России

кандидат юридических наук, доцент;

Стукалов Вячеслав Владимирович,

доцент кафедры оперативно-розыскной деятельности в ОВД

Краснодарского университета МВД России,

кандидат юридических наук

Особенности выявления фактов финансирования терроризма

В течение последних столетий терроризм проделал путь от единичных действий террористов-одиночек до высокой организованности не только в одной стране, но и на международном уровне. По данным экспертов, в настоящее время в разных странах мира насчитывается более 100

¹ Евтушок, В.П. Правовые и организационные основы оперативно-розыскной тактики: автореф. дис. ... канд. юрид. наук. – М., 1999. – 18 с.

крупных террористических организаций, поддерживающих между собой постоянные контакты.

Активизация насильственных проявлений в обществе, несет в себе прямую угрозу конституционному строю, целостности и независимости государств, его суверенитету. Многие террористические акты прямо направлены против органов государственной власти и управления с целью воспрепятствовать их нормальной деятельности¹.

Анализ современного состояния терроризма показывает: борьба с этим явлением возможна лишь при условии ограничения финансовых потоков, питающих террористическую деятельность. Изучение международной практики борьбы с насильственными актами свидетельствует о том, что его финансирование со стороны отдельных государств, кредитных корпораций и частных лиц мирового сообщества вызывает серьезную озабоченность.

Экстремистские организации и террористические группы функционируют чаще всего под вывесками различного рода благотворительных международных и российских организаций, фондов, представительств и агентств. Например, в настоящее время зафиксировано около 130 организаций, прямо или косвенно поддерживающих террористов.

Отсутствие прочных оперативных позиций, слабое умение учитывать особенности межнациональных отношений не позволяют своевременно получать полную и объективную информацию о происходящих в религиозных исламских объединениях процессах, пресекать направленные на возбуждение национальной и религиозной вражды действия, противостоять распространению радикальных исламских течений.

Методы, используемые преступными организациями за рубежом, находят применение и в России. Транснациональный характер крупных организаций определяет международный характер задач их выявления и предупреждения готовящихся террористических преступлений на территориях различных государств, проведения силами различных государств операций по уничтожению функциональных звеньев террористических организаций и структур.²

В законе под «финансированием терроризма» понимается умышленное обращение денежных средств или другого имущества полностью или частично, прямо или косвенно на совершение актов терроризма, либо умышленное накопление денежных средств или иного имущества с той же целью.

Вместе с тем, в вопросах борьбы с финансированием терроризма имеются некоторые проблемы правового и сугубо технического характе-

¹ Литвинов Н.Д. Террористические организации: формирование и деятельность: (Политико-правовой анализ): монография. - М.: 1999. - С. 11.

² <http://www.belui.ru/index.php/izdaniya-instituta/58-izdaniya-instituta/702-izdaniya-2009-g>

ра, которые требуют своего дальнейшего разрешения (например, конфискация имущества юридических лиц и другие меры).

Таким образом, борьба с терроризмом должна начинаться со своевременного выявления и перекрытия его финансовых источников, то есть по существу речь идет об изначальной профилактике терроризма. Политические мотивы в деятельности террористов тесно переплетаются с конкретными меркантильными интересами, поэтому без крупной финансовой поддержки они не в состоянии решать поставленные перед ними задачи. Экономическая основа такой поддержки — криминальные доходы, «отмытые» через различные международные финансовые институты, что и является главной причиной мировой и региональной нестабильности.

В рамках террористической деятельности в борьбе с финансированием терроризма необходимо предпринять следующие шаги:

- в целях активизации и ускорения обмена оперативной информацией, целесообразно создать международную базу данных о лицах и структурах, оказывающих финансовую поддержку терроризму, а также о методах оказания такой поддержки;

- необходима организация регулярного обмена информацией об источниках контрабандного ввоза и вывоза валюты, а также о таможенных и иных правонарушениях в оффшорных зонах;

- проведение встречных проверок экспортно-импортных контрактов в целях предотвращения хищений валютных средств и сокрытия их в иностранных банках;

- разработка механизма обмена информацией между соответствующими правоохранительными органами различных стран в отношении всех видов банковских операций по возбужденным уголовным делам и проводимым проверкам;

в центре внимания должна оставаться проблема взаимопроникновения и сращивания международного терроризма, наркобизнеса и транснациональной организованной преступности, так как у этих опасных явлений схожие, а порой и общие каналы финансовой поддержки.

Как нам известно, терроризм имеет и экономические корни, поскольку возможность осуществления террористических акции напрямую зависит от источников их финансирования, в основе которых зачастую лежат экономические преступления. Определяя механизм финансирования террористической деятельности, можно выделить следующие характерные черты экономических преступлений, в результате которых финансируются террористические организации:

- внешняя неприметность (маскировка) преступного характера деловых цепочек и механизмов совершаемых финансовых операций;

- внешняя законность каждого отдельного, обособленного действия или операции;

- частое участие в них лиц без криминального прошлого;

наличие высокопоставленных для конкретного региона должностных лиц – покровителей, как правило, прямо или косвенно корыстно заинтересованных в успешности этих криминальных операций, содействующих или скрыто руководящих осуществлением этих операций, а также препятствующих в случае вмешательства правоохранительных органов.

Касаясь финансовых условий терроризма, следует отметить тот факт, что в настоящее время террористические объединения активно используют банковский сектор. Для получения денежных средств могут быть открыты специальные коммерческие банки, цель создания которых и состоит в получении средств для поддержания терроризма. Внешне коммерческий банк выполняет свойственные ему функции, в частности аккумулирует временно свободные денежные средства. В этом нет ничего противозаконного. Однако дальнейшее размещение привлеченных средств может быть нацелено на финансирование террористических организаций. В некоторых случаях, не создавая специальные банки, террористы могут использовать для этих целей уже существующие банковские учреждения, не имеющие криминальной направленности – путем незаконного получения кредита, получения льготных условий кредитования через предоставление ложных финансовых сведений, незаконное получение государственного целевого кредита и других операций.

Помимо банков, во многих странах мира также действуют различные партии, движения, центры, коммерческие предприятия, фонды и другие организации, оказывающие всевозможную материальную и финансовую поддержку экстремистам. Справедливости ради необходимо отметить, что на территории Азербайджанской Республики действуют многочисленные международные организации, которые создают условия для осуществления финансовых операций.

Рассмотрим поэтапную деятельность следователя и оперативного сотрудника по раскрытию и расследованию финансирования терроризма.

1. Получение первичной информации:

а) от конфиденентов (лиц, оказывающих сотрудничество и содействие оперативным аппаратам на конфиденциальной основе);

б) в результате поисковой деятельности (проводится непосредственно сотрудником и опосредованно — через другие подразделения правоохранительных органов, например экономической безопасности и противодействия коррупции, отделы борьбы с незаконным оборотом наркотиков, подразделения по борьбе с организованной преступностью (во многом успех этой деятельности зависит от уровня подготовки сотрудника, а именно необходимо знание порядка функционирования финансово-кредитной системы, нормативной регламентации гражданско-правовых сделок и финансовых операций, процедуры их отражения в бухгалтерской и статистической отчетности);

в) от правоохранительных и иных государственных органов (Например, Государственный налоговый комитет Азербайджанской Республики является субъектом оперативно-розыскной деятельности, поэтому может предоставить информацию о налоговых преступлениях, прямые или косвенные сведения о совершении действий по отмыванию доходов, сведения о доходах и расходах физических и юридических лиц и т.п.);

г) от иных источников (к иным источникам относятся сообщения граждан, организации, публикации средств массовой информации).

2. Проверка первичной информации и оперативная разработка.

Функциями первичной проверки являются:

выявление и пресечение дезинформации;

выделение достоверной информации;

определение в общем массиве сведений оперативно значимой информации;

приобретение дополнительной информации, дающей основания для заведения дел оперативной разработки или возбуждения уголовного дела.

При проверке первичной информации проводятся оперативно-розыскные мероприятия, не требующие привлечения большого количества сил и средств (опрос, наведение справок, отождествление личности, наблюдение и другие действия). Неподтверждение полученной первоначальной информации влечет прекращение поисковых и проверочных мероприятий в данном направлении (не подтверждается версия о финансировании терроризма), что, однако, не исключает осуществление оперативного поиска в сфере противоправных деяний, так как признаки финансирования в ряде случаев могут совпадать с поисковыми признаками других преступлений.

Задачей оперативной проверки являются установление механизма осуществления преступной деятельности в целом: источник происхождения денег (наиболее существенный момент), преступные связи террористической группы обеспечения, способы передачи денег (конкретные виды финансовых операций и гражданско-правовых сделок), круг лиц, задействованных в подготовке и совершении преступления.

3. Реализация оперативных материалов и возбуждение уголовного дела.

Наиболее важным требованием к реализации оперативных материалов по преступлениям, как это предусмотрено ст. 214.1 УК Азербайджанской Республики (финансирование терроризма), является взаимодействие конкретного органа с другими правоохранительными органами и сотрудничество с коммерческими и иными организациями. Например, может проводиться оперативная комбинация по легализации информации о преступной деятельности по финансированию терроризма путем убеждения администрации коммерческого банка направить сообщение о подозри-

тельности сделки в правоохранительные органы, которое послужит основанием для возбуждения уголовного дела.

Можно выделить следующие варианты легализации материалов:

а) реализация начинается с проведения дополнительных оперативно-розыскных мероприятий, позволяющих возбудить уголовное дело;

б) вынесение постановления о возбуждении уголовного дела по результатам:

- задержания с поличным;
- явки с повинной;
- задержания одного из участников преступной группы по подозрению в совершении другого преступления.

Особо важным является установление момента реализации. Проведение реализации должно быть своевременным, то есть, во-первых, не являться преждевременным, когда преступная деятельность недостаточно задокументирована, и, во-вторых, не быть запоздалым, когда преступники скрылись, уничтожили следы преступной деятельности, совершили новое, преступление и т.п.

Реализация намечается и проводится:

1. Когда предмет доказывания по уголовному делу наиболее полно совпадает с предметом документирования по делу оперативной разработки, а недостающую информацию можно получить следственным путем либо в ходе оперативного сопровождения расследования.

2. Задокументированы не все преступные действия, но разрабатываемые лица пытаются совершить иное преступление – перевести деньги за границу, скрыться, уничтожить документы, магнитные носители информации или другие противоправные деяния.

3. Имеется возможность задержать подозреваемых с поличным, например, при проведении оперативного эксперимента.

Рекомендуемый нами алгоритм действий следователей и оперативных сотрудников позволяет в рамках оперативной комбинации в различных криминалистических ситуациях успешно раскрывать и расследовать факты финансирования терроризма.

Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Некоторые проблемы борьбы с распространением наркотических средств через сеть Интернет

Наркотики – это одна из главных проблем человечества. Тяга к наркотикам появляется буквально после первого потребления, приводя к физической и психологической зависимости. Также наркомания отрица-

тельно влияет и на социально-экономическое состояние страны, на духовную жизнь общества, на генофонд народа, приводит к распространению смертельно опасных заболеваний, к увеличению числа преступлений. К сожалению, статистика по заболеванию наркоманией растёт, не смотря на все возможные попытки борьбы. Реальное число наркопотребителей в России оценивается международными экспертами в 18 млн. человек, 8 млн человек употребляют их постоянно. Из них молодежь до 30 лет составляет более 60 %. Пятая часть – это школьники, которые принимают наркотики с 9–13 лет. Число наркоманов, состоящих на медицинском учете на июнь 2017 составлял 800 тыс. человек¹.

Помимо статистики заболеваний растёт также число преступлений, связанных с незаконным оборотом наркотических средств. По данным федеральной службы государственной статистики на территории РФ на момент января 2018 года количество преступлений, связанных с незаконным оборотом наркотиков, составляет 16920. Это только то число, которое официально зарегистрировано. Эксперты-криминалисты утверждают, что лишь одно из десяти преступлений удаётся выявить. Борьба с незаконным оборотом наркотических средств – актуальная проблема современного общества. Из-за активного применения наркотиков в медицине невозможно полностью запретить их оборот. Поэтому задача правового режима существования наркотиков: создание эффективных правовых норм для регулирования их законного оборота и использования².

Какие конкретно проблемы имеются при борьбе с таким злом в нашей стране в настоящее время?

Важную роль в распространении наркотических средств и их аналогов, информации о них среди населения играют средства массовой информации. Именно через радио, телевидение, газеты и журналы мир узнает о тех или иных вещах. Главенствующее место в современном мире по праву занимает сеть Интернет.

Ни для кого не секрет, что в последнее время стали увеличиваться случаи распространения наркотиков именно через данную «Всемирную сеть». В марте 2012 года статья 228.1 УК РФ была дополнена квалифицирующим признаком сбыта наркотических средств, психотропных веществ их аналогов при помощи СМИ. Ее пункт «б» гласит «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет)». При такой форме «Всемирная сеть» применяется в качестве рекламы или предложения сбыта наркотических средств, для указания тайников, где они в данный мо-

¹ Сайт государственная статистика РФ <http://www.gks.ru/>

² Проблемы борьбы с наркоманией и незаконным оборотом наркотических средств и психотропных веществ требуют программно-целевого подхода и эффективных законодательных мер. - (Электронный ресурс). - Режим доступа URL: <http://www.buroadvokat.ru> (дата обращения: 22.11.2017).

мент находятся, время их извлечения, получения информации об оплате за приобретение. Так, на большинстве популярных наркотических сайтов существуют «чат-комнаты»-интерактивные странички, с помощью которых осуществляется общение в реальном времени на волнующие наркозависимых темы (цена, какое действие на организм после употребления, где купить и т.д.). С помощью социальных сетей, электронной почты осуществляются различные тематические сетевые конференции, на которых происходит общение без каких-либо ограничений. Сотрудники МВД выявили около 9,5 тысяч интернет-сайтов, через которые преступные группы могли распространять наркотики, сообщил начальник Главного управления по контролю за оборотом наркотиков МВД России Генерал-лейтенант Храпов Андрей Иванович¹.

Также популярностью пользуются мессенджеры, такие как WhatsApp, Telegram, Viber. Во всех странах разработчики мобильных приложений в сфере телекоммуникации стараются максимально защитить передаваемую там информацию, сохранить приватность переписок. Из-за этого правоохранительные органы упускают информацию, которая на стадии предварительного или судебного следствия могла бы стать важным доказательством причастности лиц к преступной деятельности. Серьезный алгоритм защиты информации у недавно созданного мессенджера Telegram. В нем имеется функция «секретный чат», где сообщения удаляются автоматически, если пользователи установят удобное время, на серверах приложения переписки также не сохраняются.

Но это не сравнится с особой системой анонимайзеров, в том числе VPN и наиболее распространённой TOR. Для перевода денежных средств используются электронные платежи WebMoney, QIWI-кошелек, RuPay, Cybercash, «Яндекс. Деньги» и с недавних пор стали расплачиваться цифровыми деньгами (биткоин и другие криптовалюты). Они бывают анонимные (неперсонифицированные), разрешающие проводить операции без идентификации пользователя, ими естественно и пользуются преступники.

Что же собой представляет Система TOR? Это анонимная сеть виртуальных туннелей, где происходит передача информации в зашифрованном виде. В целом эта система весьма сложная и запутанная, поэтому создаёт отличную защиту от слежения со стороны властей. После 2002 года, когда был запущен TOR, вышло его несколько усовершенствованных версий, где сужались возможные лазейки для «раскрытия» пользователей. Первые русскоязычные сайты в зоне onion сети TOR появились ещё в 2012 году.

По статистике МВД, количество осуждённых за хранение и распространение наркотиков в крупном/особо крупном размере возросло с 34 ты-

¹ Пресс – конференция руководителя ГУНК МВД России 27.09.2016 года. [Электронный ресурс] / Пресс-центр МВД России. – 2016. – URL: <http://izvestia.ru/news/634748#ixzz4MxdYk5an> (дата обращения: 12.11.2017).

сяч человек в 2012 году до почти 45 тысяч в 2014 году¹. Именно поэтому большое количество преступников предпочло вести свой незаконный бизнес в сети Интернет. По данным TOR Metrics, Россия на втором месте после США по числу пользователей «теневого» интернета. В 2015 году органы власти активно взялись за инициативу по борьбе с использованием анонимайзеров и «луковичной» сети TOR. Правительство и контролирующий орган пытаются объявить анонимные сети вне закона и полностью ограничить к ним доступ, так как считают это притоном преступников. Но несмотря на все усилия властей, этого сделать пока не удалось.

Для того, чтобы изобличить преступников потребуется много сил, средств и времени. В первую очередь за подозреваемым следят в сети, параллельно отрабатывая круг его общения и клиентскую базу. Иногда даже на этой стадии удаётся распознать IP-адрес преступника, если в его действиях были допущены ошибки. А уже после этого устанавливается адрес злоумышленника и происходит задержание.

Как только данные покидают стены TOR, они сразу становятся незащищенными, уязвимыми, что, в свою очередь, подразумевает, что сайт, доступ к которому стремятся получить, может быть заблокирован и отслеживаться, и, если преступник направляет какую-либо информацию другим лицам, они также попадут в поле зрения специальных служб, которые осуществляют мониторинг. Также создаются подставные ресурсы, форумы и ссылки, на них размещают изображения и видео, часть которых располагается в другой доменной зоне – например, com или ru. Файлы открываются вне TOR-браузера, и защитники правопорядка сразу вычисляют настоящий IP-адрес преступника.

Как квалифицируются данные преступления? Все виды рекламы и предложений сбыта через Интернет квалифицируют, как подготовительную стадию сбыта. Для этого необходимо установить у лица прямой умысел на сбыт и совершение лицом действий, которые были направлены на реализацию умысла. Когда лицо направляется с наркотическими средствами к месту тайника, чтобы их там оставить и после сообщить через «всемирную сеть», вменяют приготовление к сбыту наркотических средств с использованием сети Интернет. Преступные сообщества, которые создаются с целью сбыта наркотических средств через сеть Интернет, отличаются следующими ролями его участников:

Организатор – руководит преступным сообществом по приобретению, производству, фасовке наркотиков. Занимается распределением доходов.

Диспетчер- принимает заказы, передаёт нужную информацию кладчикам и курьерам и информирует их о местонахождении тайников.

¹ Сайт статистика МВД <https://мвд.пф/Deljatelnost/statistics>

Специалист в сфере компьютерных технологий- организывает техническую деятельность сетевых ресурсов, занимается конспирацией участников преступной группы в сети Интернет и мобильных приложений связи, а также при получении доходов на электронные и банковские счета.

Вербовщик – ищет и вовлекает в преступную деятельность новых участников.

Курьер – фасует, перевозит наркотики и передаёт их закладчику в основном небольшими партиями.

Закладчики – создают тайники («закладки») для покупателей и передаёт информацию диспетчеру.

Данное иерархичное построение исключает личное знакомство его участников. Низшие звенья (курьер и закладчик) не имеют информации о более высоких участниках. Бывает, что они находятся на больших расстояниях от друг друга, в том числе разных странах, что непосредственно усложняет работу правоохранительных органов.

Таким образом, мы постарались охватить наиболее проблемные вопросы борьбы с оборотом наркотических средств в настоящее время. Экспертами подтверждено, что именно информация посредством «Интернет» – сильный и действенный метод распространения наркомании.

Какие меры борьбы мы предлагаем?

1. Самый эффективный способ-усовершенствование и ужесточение мер уголовно-правового воздействия, усиление контроля за соблюдением законодательства в сфере телекоммуникационных сетей и мобильных приложений.

2. Создание в отделах уголовного розыска (ведь именно он занимается выявлением фактов сбыта наркотических средств) отделения, непосредственно занимающегося расследованием преступлений через «интернет». Людей, обладающими высочайшими специальными познаниями в этой области. Которые бы анализировали текущее состояние наркопреступности в киберпространстве, идентифицировали лиц, которые причастны к данным видам преступлений, путём отслеживания подозрительных потоков денег, почтовых/телеграфных отправок.

3. Продолжать блокировать различные сайты, где осуществляется размещение информации о наркотических средствах, внесение их в реестр запрещённых Интернет-ресурсов. Так как создание сайта по распространению наркотиков- дело не затратное и быстрое, поэтому с каждым днём появляются новые и для выявления их существования необходимо немало времени.

4. Ограничить возможность доступа в системы анонимайзеров.

5. Исключить возможность создания любых сайтов без внесения достоверных персональных данных, для того, чтобы правоохранительные органы смогли идентифицировать личности преступников, также чтобы свести на минимум создание анонимных сайтов, соединений, чатов и т.д.

6. На международном уровне необходимо упростить процедуры межгосударственного сотрудничества правоохранительных органов. Нередко используемые Интернет-ресурсы находятся вне территории России (США, Китай, страны Европы и т.д.), но могут возникать проблемы территориальной юрисдикции государств. Целесообразно образовать межгосударственную комиссию для обмена нужной информацией и дальнейшего выявления преступных организаций, осуществляющих незаконный оборот наркотиков на территории данных государств.

Проблема незаконного сбыта наркотических средств с использованием телекоммуникационных систем и устройств была и остаётся актуальной, требует правильного решения на законодательном уровне, разработки специальных методик раскрытию преступных организаций в данной области.

Усманова Назиля Мунировна,
Курсант Казанского института МВД России;
Усманов Ильгиз Миншакирович,
доцент кафедры оперативно-разыскной деятельности
Казанского юридического института МВД России,
кандидат юридических наук

Совершенствование оперативно-розыскных мероприятий в сфере противодействия незаконному обороту наркотиков бесконтактным способом

Состояние здоровья населения является важным показателем уровня развития государства, одним из основных факторов развития общества, поэтому охрана здоровья населения есть одна из первостепенных задач. Охрана здоровья людей, несомненно, представляет стратегическую задачу в успешном формировании и развитии будущего нашего государства. В настоящее время в демографических показателях сохраняется депопуляция и естественная убыль населения, ухудшение показателей здоровья, сокращение продолжительности жизни.

Распространение наркотических средств и психотропных веществ, представляет собой реальную угрозу здоровью не столько отдельного индивида, сколько здоровью населения и человечеству в целом.

В Государственной программе Российской Федерации «Противодействие незаконному обороту наркотиков» отмечается, что одной из основных проблем незаконного оборота наркотиков в России является использование сети Интернет в целях пропаганды немедицинского потребления наркотиков, их производства и распространения.¹

¹ См.: Об утверждении государственной программы Российской Федерации «Противодействие незаконному обороту наркотиков»: Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 299 // Собрание законодательства Российской Федерации. –2014. – № 18. – Ст. 2148.

На сегодняшний день экспансия наркотических средств на территории Российской Федерации носит эпидемический характер. Безусловно, одним из факторов такого проявления является относительная доступность наркотиков, которые распространяются путем массовой рассылки сообщений абонентам сети сотовой связи; «наружной рекламы» (на заборах, подъездах и т.п.), через объекты розничной торговли; через сеть Интернет; в местах массового скопления людей (в виде листовок на вокзалах, аэропортах, станциях метрополитена); в кальянных и др.

За последние годы русскоязычная часть Интернета оказалась переполнена сайтами, предоставляющими информацию о рецептуре изготовления, приспособлениях для потребления наркотиков, психоделических переживаниях, возможных негативных эффектах вследствие употребления подобных препаратов и преодолении абстинентного синдрома.

На наш взгляд, следует обратить особое внимание на использование преступником анонимных и конфиденциальных сетей Интернет, посредством которых создаются онлайн магазины по продаже наркотиков. Одной из таких сетей является «Тор». Это одна из самых популярных анонимных сетей, основанная на «луковой» маршрутизации. Клиенты сети «Тор» формируют виртуальные соединения, состоящие из двух или более узлов, которые передают трафик пользователя на конечный сервер. Их данные шифруются несколько раз перед передачей через сеть «Тор» таким образом, чтобы исходная информация была доступна только на выходном узле (последнем узле в маршруте). Система позволяет устанавливать анонимное сетевое соединение, защищённое от прослушивания и может рассматриваться как анонимная сеть виртуальных туннелей. Возможность контроля указанных каналов связи у правоохранительных органов крайне низкая, что является серьезной проблемой правоприменения и требует скорейшего разрешения.

На созданном преступниками ресурсе размещается рекламное описание предлагаемых для реализации наркотических средств. Форма подачи материала при этом может быть различной вплоть до описания состояния после употребления товара. Также покупателю предоставляется возможность использования электронной корзины для упрощения составления заказа. В процессе оформления потребителю предоставляется выбор способов оплаты и получения заказа (Web-Money, Яндекс-Деньги и др.). После осуществления платежной транзакции покупателю направляется сообщение с указанием места нахождения тайника с наркотиками. В отдельных случаях после оплаты преступники отправляют потребителю посылку с наркотиком обычной почтой или курьерскими службами на адрес, указанный в заявке. По вышеуказанной системе работает множество магазинов, например, такие как «Nice Guy», «Silk Road», «Shama shop». Следует отметить, что отсутствие непосредственного контакта преступников с потребителем при передаче наркотика в подобных случаях исключает применение

оперативными сотрудниками хорошо отработанных на практике тактических оперативно-розыскных алгоритмов установления участников.

Соответственно, перед правоохранительными органами, в том числе и перед оперативными подразделениями ОВД, четко поставлена задача выявлять и изобличать лиц, распространяющих наркотики с использованием инфокоммуникационных технологий. На практике решению этой задачи препятствует ряд обстоятельств, среди которых особо выделяется необходимость привлечения к указанной деятельности значительного количества сил и средств, главным образом со стороны подразделений, осуществляющих оперативно-технические мероприятия. Тем не менее, правильно организованное наблюдение за сетевыми ресурсами в Интернете и грамотное проведение в сети комплексных оперативно-розыскных мероприятий все чаще позволяют оперативным сотрудникам выявлять и задерживать поставщиков наркотических средств. Например, в 2015 г. Сотрудниками ФСКН России, в ходе проведения совместной международной операции с китайскими и испанскими коллегами под кодовым названием «Мозаика», был задержан гражданин Ситников А., который, будучи организатором преступной группы, занимался сбытом наркотиков синтетического происхождения через созданный и моделируемый им интернет-магазин. В сделках участвовали клиенты из Соединенных Штатов Америки, Латинской Америки, ряда европейских стран, Австралии и Азии. При этом в большинстве случаев отследить пути заказчиков и продавцов было крайне затруднительно, так как обе стороны пользовались анонимной системой «Тор».

На первоначальном этапе выявления рассматриваемого вида преступлений особое значение приобретает поиск первичной оперативной информации в сети Интернет и ее проверка, проведение которых предполагают наличие у оперативного сотрудника специальных знаний и умений.

После выявления ресурсов, через которые организован оборот наркотических средств, важно обеспечить установление контакта с продавцами. В рамках проведения оперативно-розыскной деятельности необходимо использование такого мероприятия как «Наведение справок». С помощью него выясняются способы связи с продавцами и данные контактов, в том числе номеров мобильных телефонов, электронных кошельков, банковских счетов и т.п. Наведение справок позволяет установить лиц, на которых они зарегистрированы, собрать максимальное количество информации о них. Также запрос по счету электронного кошелька позволит узнать анкетные данные, предоставленные при его регистрации, даты и суммы пополнения установленных счетов терминала оплаты с указанием адресов их местонахождения, переводы средств оплаты на иные счета с указанием номеров, даты, времени и суммы перевода, а также информацию о получении денежных средств (Ф.И.О., дата рождения, вид, номер и дата выдачи документа удостоверяющего личность, адрес места житель-

ства получателя), телефоны, указанные держателем номера, на которые могут приходиться SMS-оповещения о проведенных операциях по счету. Кроме того может понадобиться информация об адресе электронной почты и IP-адресе, с которого осуществлялась регистрация и IP-адреса, с которых осуществлялись входы на него. Важно принять меры к определению физического местонахождения устройств, с помощью которых преступниками осуществляется выход в сеть Интернет.

Для установления держателя электронного кошелька необходимо проанализировать, возможную оплату им каких-либо иных покупок или услуг. Например, оплату услуг сотовой связи, услуг провайдера Интернета, услуг сайта знакомств и т.д. В дальнейшем легендированный запрос в компанию, осуществившую какие-либо услуги, позволяет установить анкетные данные фигуранта.

Нельзя также исключить, что фигуранты переводят денежные средства на другие мобильные кошельки, привязанные к номерам сотовых телефонов. В таком случае для получения информации о движении денежных средств по счету необходимо проведение ОРМ «Снятие информации с технических каналов связи — СМС».

Проанализировав полученную информацию предоставляется возможность установить «диспетчера» сети сбыта (владельца электронного кошелька), «закладчиков» (владельцев других счетов, которым перечисляются небольшие суммы оплаты за их услуги), а также вышестоящие звенья сети (владельцев банковских карт, которым регулярно перечисляются более крупные суммы оплаты), с учетом того, что, как правило, многие банковские карты привязываются к номерам мобильных телефонов.

В дальнейшем необходимо организовать взаимодействие с сотрудниками подразделений специальных технических мероприятий, в ходе которого:

- провести ОРМ «Снятие информации с технических каналов связи» — определение местонахождения абонента владельца номера мобильного телефона;

- направить запрос на установление анкетных данных владельцев номеров мобильных телефонов;

- провести СИТКС по номерам мобильных телефонов, в том числе по установлению их imei, их активность, привязки к базовым станциям;

- поставить на контроль телефонные переговоры фигурантов по выявленным номерам (ОРМ «Прослушивание телефонных переговоров»)

- провести СИТКС по SMS и иным сообщениям, направляемых с мобильных телефонов проверяемых или разрабатываемых фигурантов

- поставить на оперативный контроль телефонные переговоры и SMS-сообщения, ведущиеся с номера, указанного в рекламе сбыта наркотиков.

Весь период оперативной проверки или разработки целесообразно осуществлять постоянное взаимодействие с подразделениями оперативно-

разыскной информации территориальных и других органов МВД России. Тем самым, в ходе соответствующего аналитического поиска можно выявлять и получать дополнительную оперативно-значимую информацию.

После того как основные участники организованной преступной группы установлены и их преступные действия надлежащим образом зафиксированы, следует переходить к реализации материалов оперативной разработки и задержанию фигурантов. При наличии благоприятно складывающейся оперативно-тактической ситуации участники преступной группы должны быть задержаны почти одновременно.

Исходя из всего вышеизложенного предлагается проводить оперативно-розыскной мониторинг сетевого пространства, а именно анонимных и конфиденциальных сетей. Не исключается также возможность проведения оперативного внедрения в рассматриваемые криминальные структуры для получения большей информации и способствованию закрытию нелегальных Интернет-магазинов. Для осуществления данных мер, несомненно, необходима организация подготовки кадров, осуществляющих специфические задачи по противодействию преступности в киберпространстве. Для такой подготовки необходимо создание новой материально-правовой базы, организация научных исследований, результатом которых должны стать методические рекомендации по эффективному осуществлению оперативно-розыскной деятельности в сети.

Разумеется, это далеко не исчерпывающий перечень мер, способствующий повышению эффективности проведения оперативно-розыскных мероприятий в сфере противодействия незаконного оборота наркотических средств через Интернет-ресурсы. Однако, на наш взгляд, они существенно повлияют на улучшение наркоситуации в нашей стране.

Ховавко Сергей Михайлович,
доцент кафедры оперативно-розыскной деятельности
и специальной техники Крымского филиала
Краснодарского университета МВД России,
кандидат юридических наук

Использование технологии распознавания лиц в оперативно-розыскной деятельности

Решение задач оперативно-розыскной деятельности в подавляющем большинстве случаев требует от оперативных подразделений установления личности или местонахождения лиц, подготавливающих, совершающих или совершивших преступления, лиц, находящихся в розыске, потерпевших и свидетелей преступлений и других категорий лиц. С этой целью оперативные подразделения уполномочены проводить оперативно-

розыскные мероприятия, исчерпывающий перечень которых содержится в ст. 6 ФЗ «Об ОРД»¹. Технология распознавания лиц в оперативно-розыскной деятельности, на наш взгляд, может наиболее эффективно использоваться при осуществлении оперативно-розыскного мероприятия отождествление личности.

Отождествление личности, в соответствии с ведомственными нормативными актами органов внутренних дел, – это оперативно-розыскное мероприятие, которое заключается в установлении и идентификации лица по индивидуализирующим статическим и динамическим неизменяемым признакам, а также при помощи других способов, позволяющих с достаточной степенью вероятности опознать его личность. Отождествление личности относится к мерам проверочного характера с целью установления лиц, причастных к преступной деятельности, путем непроцессуального опознания по идентифицирующим признакам, а также для решения задач оперативно-розыскной деятельности, связанных с розыском лиц.

По мнению В.И. Шарова, в теории оперативно-розыскной деятельности сложились две позиции по определению сущности отождествления личности. Первая позиция (А.Ю. Шумилов и др.) сводится к пониманию отождествления как опознания людей по мысленному образу (внешности, голосу, следам запаха), материальным отображениям (фотографиям, видео- и аудиозаписям). Сторонники второй позиции К.К. Горяинов, К.К. Кваша, К.В. Сурков кроме опознания включают в данное оперативно-розыскное мероприятие исследование предметов, документов, биологических объектов, фотоснимков, видео- и аудиозаписей.²

В развитие идеи, предложенной А.Ю. Шумиловым, интерес представляет классификация видов отождествления личности, сформулированная В.М. Шикановым, который выделяет отождествление по признакам внешности, отпечаткам пальцев рук, почерку и письменной речи; по голосу и устной речи; по биологическому материалу и выделениям человека (метод ДНК-анализа).³

Наиболее часто при раскрытии неочевидного преступления проводятся следующие виды рассматриваемого оперативно-розыскного мероприятия: демонстрация фото- или видеоизображений поставленных на учет лиц; совместное с потерпевшим, свидетелем патрулирование (поиск)

¹ Об оперативно-розыскной деятельности : федеральный закон от 12.08.1995 № 144-ФЗ. – URL: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW;n=181943> (дата обращения: 05.11.2017).

² Шаров В.И. Понятие и виды отождествления в ОРД / В.И. Шаров // Проблемы оперативно-розыскного обеспечения уголовного судопроизводства в уголовно-процессуальном стимулировании оперативно-розыскной деятельности: сб. ст. – Н.Новгород: Нижегор. акад. МВД России, 2010. – С. 318 – 328, с. 319

³ Шиканов В.М. Отождествление личности в системе оперативно-розыскных мер обеспечения экономической безопасности / В.М. Шиканов // Вестн. Нижегор. акад. МВД России. – 2009. – № 2 (11). – С. 112 – 117, с. 113-114

преступника в местах наиболее вероятного его появления; отождествление личности с применением служебно-розыскной собаки.

В соответствии с ч.3 ст.6 ФЗ «Об ОРД» в ходе проведения оперативно-розыскных мероприятий (в т.ч. при отождествлении личности) используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.¹ К одним из таких иных средств, на наш взгляд, можно отнести активно совершенствующуюся технологию распознавания лиц, получившую в последнее время широкое распространение в различных сферах.

Технология распознавания лиц представляет из себя встроенные компьютерные программы, которые анализируют изображения лиц людей в целях их идентификации. Программа берет изображение лица и измеряет такие его характеристики, как расстояние между глазами, длина носа, угол челюсти, на основе чего создается уникальный файл, который называется «шаблон». Используя шаблоны, программа сравнивает данное изображение с другими изображениями, а затем оценивает, насколько изображения являются похожими друг на друга.

Наиболее передовой формой технологии распознавания лиц в настоящее время является программа FindFace, созданная компанией N-Tech.Lab. Сервис FindFace, разработанный для пользователей крупнейшей в России социальной сети «ВКонтакте», сможет отыскать в виртуальном пространстве любого человека всего по одной фотографии. Похожие лица выявляются по восьмидесяти признакам. Американское Агентство передовых исследований в сфере разведки (IARPA) признало российскую N-techLab (разработчика сервиса FindFace) лучшей в сфере технологий распознавания лиц.²

Обычными источниками изображений для использования технологии распознавания лиц могут являться фотографии и видеозаписи с различных технических средств (камеры наружного наблюдения различных предприятий, учреждений, организаций; ПТК «Безопасный город»; автомобильные или носимые видеорегистраторы; мобильные телефоны граждан и т.п.). Предварительное получение фото- видеоизображения для последующего отождествления личности в сети Интернет с использованием технологии распознавания лиц может осуществляться посредством проведения различных оперативно-розыскных мероприятий.

Отождествление личности в сети Интернет с использованием технологии распознавания лиц может осуществляться как самими оперативными

¹ Об оперативно-розыскной деятельности : федеральный закон от 12.08.1995 № 144-ФЗ. – URL: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW;n=181943> (дата обращения: 05.11.2017).

² Лента.Ру – URL: <https://lenta.ru/news/2017/11/08/iarpa/> (дата обращения: 05.11.2017).

сотрудниками различных оперативных подразделений, так и лицами, оказывающими содействие оперативным подразделениям по заданиям оперативных сотрудников. Использование технологии распознавания лиц в целях идентификации в сети Интернет может применяться заинтересованными гражданами (в первую очередь потерпевшими) и по собственной инициативе, результаты такого отождествления могут предоставляться сотрудникам оперативных подразделений для последующего использования в целях оперативно-розыскной деятельности.

Таким образом, активное использование социальных сетей лицами, представляющими оперативный интерес, на наш взгляд, дает основание вести речь о внедрении в практическую деятельность оперативных подразделений нового вида отождествления личности – отождествление личности в сети Интернет с использованием технологии распознавания лиц. Использование технологии распознавания лиц в оперативно-розыскной деятельности может применяться в целях установления личности лиц, представляющих оперативный интерес (подготавливающих, совершающих, совершивших преступления; лиц, находящихся в розыске; потерпевших, свидетелей преступлений).

СОДЕРЖАНИЕ

Акопов А.А., Николаева И.И. Актуальные проблемы взаимодействия следователя и оперативных сотрудников в ходе уголовного судопроизводства.....	3
Абдурагимова Д.А., Сафронов А.А. Теоретические основы и актуальные проблемы введения оперативно-розыскного мероприятия «получение компьютерной информации» в оперативно-розыскную деятельность.....	5
Айтманбетов И.М., Кислицын Н.А. Проблема доверия к сотрудникам подразделений уголовного розыска.....	9
Азаров Д.С., Стукалов В.В. Особенности санкционирования оперативно-розыскного мероприятия «получение компьютерной информации».....	11
Андреев С.Э. Некоторые способы мошенничества в строительной сфере железнодорожного транспорта.....	15
Ардавов М.М., Голяндин Н.П. О применении нетрадиционных подходов (методов) в оперативно-розыскной деятельности.....	19
Белый А.Г., Киселев С.С. Состояние оперативной обстановки в сфере противодействия экстремизму и терроризму в Северо-Кавказском федеральном округе.....	25
Бильданова Л.И. Оперативная провокация как способ фальсификации (ч. 4 ст. 303 УК РФ).....	32
Габисов С.В., Стукалов В.В. Выявление фактов мошенничества, связанных с использованием бесконтактной оплаты.....	36
Горбанев В.М., Стукалов В.В. О некоторых проблемах предупреждения и раскрытия мошенничеств, связанных с использованием средств сотовой связи.....	38
Горбунов А.Н. Основные источники угроз экстремизма в современной России.....	41
Добросмыслов А.Э., Сафронов А.А. Информационное противоборство экстремизму и терроризму в сети Интернет.....	46
Зекох А.Г. Проблемы вовлечения лиц в деятельность экстремистских организаций.....	49
Иванов С.И. Отдельные направления совершенствования оперативно-розыскной деятельности органов внутренних дел в современных условиях.....	55
Кибатов М.С., Музеев А.И. Использование специального программного обеспечения в оперативно-розыскной деятельности по противодействию преступлений, совершаемых с использованием компьютерных технологий.....	57

Киселев С.С., Белый А.Г. Угрожающие факторы экстремистских и террористических проявлений на Северном Кавказе.....	62
Кислицын Н.А. Тактика действий сотрудников оперативных подразделений в различных ситуациях оперативно-служебной деятельности.....	67
Красников В.Н. Правовые основы взаимодействия оперативных подразделений органов внутренних дел с общественностью.....	71
Молько М.Е., Стукалов В.В. Некоторые особенности выявления наркотических закладок.....	76
Петухов А.Ю. Современные информационные технологии и преступность в сфере незаконного оборота наркотиков.....	80
Пестрецов М.А. Особенности получения оперативно-розыскной информации в сети Интернет.....	84
Сафронов А.А., Стукалов В.В. Особенности выявления фактов финансирования терроризма.....	86
Стукалов В.В. Некоторые проблемы борьбы с распространением наркотических средств через сеть Интернет.....	91
Усманова Н.М., Усманов И.М. Совершенствование оперативно-розыскных мероприятий в сфере противодействия незаконному обороту наркотиков бесконтактным способом.....	96
Ховавко С.М. Использование технологии распознавания лиц в оперативно-розыскной деятельности.....	100

Научное издание

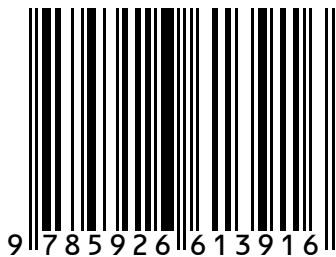
**АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
VI Международной научно-практической конференции

(24 ноября 2017 г.)

В авторской редакции
Компьютерная верстка Г. А. Артемовой

ISBN 978-5-9266-1391-6



Подписано в печать 02.10.2018. Формат 60x84 1/16.
Усл. печ. л. 6,2. Тираж 100 экз. Заказ 718.

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