Е.П. Ищенко[*], П.П. Ищенко[**]

СОВРЕМЕННЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В БОРЬБЕ С ОРГАНИЗОВАННОЙ НАРКОПРЕСТУПНОСТЬЮ

Ключевые слова: тенденции развития преступности, использование Интернета в преступных целях, организованная наркопреступность, преступное сообщество, контроль и запись телефонных переговоров, судебно-фоноскопическая экспертиза, анализ информации, уголовное дело

Оценивая изменения российской преступности, произошедшие в последние десятилетия, необходимо заострить внимание на четырех основных, тесно взаимосвязанных между собой тенденциях ее развития. Первое, что следует отметить, это изменение преступных мотиваций, которые в абсолютном большинстве случаев стали корыстными. Столь распространенное в советский период хулиганство кануло в прошлое, уступив место различным преступно-корыстным проявлениям. Во-вторых, совершение преступлений стало бизнесом, а в условиях разрастающейся глобализации, открытости общества и «прозрачности» границ – бизнесом меж-

© Ищенко Е.П., 2012

[*] Доктор юридических наук, профессор, заслуженный деятель науки РФ, заведующий кафедрой криминалистики Московской государственной юридической академии имени О.Е. Кутафина. [kriminalistmsal@list.ru]

[**] Кандидат юридических наук, заместитель начальника Следственного управления Следственного департамента ФСКН России.

дународным и трансграничным, сориентированным на получение сверхдоходов.

Прямым следствием этого явилось резкое повышение уровня организации преступной деятельности. Современная преступность, будь то торговля наркотиками или контрафактными товарами, рейдерство или «финансовые пирамиды», является сложно организованным криминальным «предприятием», объединяющим десятки, а то и сотни участников. Четвертой характерной чертой, определяющей суть современной российской преступности, представляется высокая техническая оснащенность криминалитета.

Это качество является как следствием «импорта» преступных технологий из-за рубежа (вместе с техническими новинками и услугами), так и вооружения «традиционной» преступности современными техническими средствами и технологиями. Не только в обществе в целом, но и в преступной среде наибольшие изменения вызваны распространением общедоступных коммуникационных технологий, в частности таких, как Интернет и мобильная связь. Последняя, как известно из кибернетики, составляет необходимое условие любой организации.

Осмысление сущности Интернета позволяет заключить, что необходимо рассматривать его как некий феномен, оказывающий непосредственное влияние на характер и структуру современной преступности. В качестве такового он обладает рядом специфических свойств, анализ которых позволяет глубже понять криминологические и криминалистические проблемы расследования и предупреждения сетевых и связанных с использованием IT-технологий преступлений. Наиболее значимыми среди них, на наш взгляд, необходимо назвать следующие:

1. Надгосударственный и децентрализованный характер Интернета, отсутствие единой организации, полностью координирующей и контролирующей его функционирование, очень затрудняет осуществление в глобальной сети правоохранительной деятельности. В большинстве стран, в том числе и в России, система регулирования и контроля Интернета находится в стадии становления.

2. Технологическая незащищенность глобальной сети, которая изначально создавалась как открытая среда коммуникации исследовательских и военных компьютерных центров. Тогда даже не предполагалось, что кто-то вознамерится использовать Интернет в преступных целях.

3. Возможность анонимной деятельности в глобальных компьютерных сетях, упрощенные процедуры регистрации пользователей провайдерами, практически полное отсутствие достоверных идентификаторов личности при работе в Интернете существенно затрудняют выявление лиц, совершающих сетевые преступления, особенно трансграничные.

4. Влияние глобальных компьютерных сетей на состояние национальной безопасности многих технологически развитых государств способно приводить к попыткам блокирования важных сетевых объектов со стороны различных правонарушителей.

Указанные факторы, перечень которых, увы, не является исчерпывающим и может быть существенно расширен, усугубляются неразвитостью теоретических и правовых основ противодействия преступным посягательствам в Интернете и механизмов их реализации.

В этой связи становится понятным, почему представители «традиционной» общеуголовной преступности так быстро осознали те преимущества, которые им предоставляет Интернет (различные виды мошенничества, распространение детской порнографии, запрещенных товаров и услуг). Не отстали от них и представители хакерского сообщества, занявшиеся взломами зарубежных и отечественных серверов, хищениями информации, блокированием работы сетевых объектов и другими атаками на глобальную сеть. Организованная преступность все активнее привлекает две первые категории лиц для достижения своих противоправных целей[1].

Характеризуя современную организованную наркопреступность, необходимо признать, что все названные выше тенденции проявились в ней более ярко и отчетливо, чем в какой-либо иной сфере криминальной деятельности. Под этим углом зрения весьма актуальной представляется проблема выявления, расследования и судебного рассмотрения уголовных дел данной категории. Суть проблемы для практических работников достаточно очевидна: количество выявленных преступлений, предусмотренных ст. 210 УК РФ, явно не соответствует уровню организованности современной наркопреступности, а количество судебных приговоров с этой квалификацией – и того меньше. Может создаться впечатление, что преступным наркобизнесом занимаются чуть ли не одиночки.

При системном подходе к рассмотрению данного вопроса разумно предположить, что проблема едва ли локализована в каком-то одном звене «технологической цепочки» средств и методов борьбы с наркопреступностью: в криминалистике, в судебной экспертизе, в оперативно-розыскной деятельности, в уголовном процессе или праве, либо в какой-то области смежного законодательства. Вероятнее всего, что решение проблемы повышения эффективности борьбы с организованной наркопреступностью частично сосредоточено в каждой из перечисленных сфер практической деятельности правоохранительных органов. Соответственно, устранение сбоев в любом «звене» этой «цепочки» должно положительно сказаться на общем результате борьбы с наркотрафиком.

Так, введенные в действие Федеральным законом от 3 ноября 2009 г. № 245–ФЗ новые редакции ст. 35 и 210 УК РФ, а также разъяснения, данные Пленумом Верховного Суда Российской Федерации в постановлении от 10 июня 2010 г. № 12 «О судебной практике рассмотрения

[1] См. подробнее: *Осипенко А.Л.* Трансграничные преступления, совершаемые с использованием сети Интернет // Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы информационной безопасности. Вып. VII. Калининград, 2006. С. 232–247.

уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)», устранили существовавшие ранее неточности в конструкции названных норм. Из закона и из юридической практики исключен такой признак преступного сообщества (преступной организации), как «сплоченность».

Субъективное и нечеткое содержание этого признака создавало своего рода «юридический люфт», обуславливавший непроизвольное «сползание» квалификации в процессе судебного рассмотрения уголовного дела от преступного сообщества к менее тяжкой форме групповой преступности – организованной группе. Сегодня этот вопрос решен. Введенный законодателем признак структурированности вполне объективен и доказуем. Содержанию данного признака дано четкое определение в разъяснениях Пленума Верховного Суда РФ.

Результат не замедлил сказаться: если в 2009 г. из 29 оконченных Следственным департаментом ФСКН России дел данной категории лишь в 8 случаях (27,6 %) квалификация содеянного по ст. 210 УК РФ получила подтверждение в приговоре, то в 2010 г., по результатам рассмотрения 41 расследованного дела, квалификация по данной статье Уголовного кодекса «устояла» уже по 23 делам (56,1 %), т.е. возросла более чем в 2 раза. Приведенные данные убедительно подтверждают выдвинутый тезис и указывают на необходимость оптимизации других «звеньев технологической цепочки».

Успехи правоохранительных органов в борьбе с организованной преступностью в современных условиях прямо и непосредственно зависят от своевременного прогнозирования криминогенных последствий внедрения в общественную жизнь новых технических средств и технологий, а также связанных с ними услуг. В этом контексте очень важна разработка надежных методов выявления и фиксации криминальной активности, способов формирования судебных доказательств, построения систем доказывания при расследовании и судебном рассмотрении уголовных дел анализируемой категории. Наиболее пристального внимания в указанном аспекте заслуживают общедоступные информационно-коммуникационные технологии, переживающие в своем развитии настоящий «бум».

Так, появление около 20 лет назад средств мобильной телефонной связи и ее последующее очень широкое распространение среди всех слоев населения существенно повлияло и на организованную преступность, и на методы работы правоохранительных органов. Мобильный телефон, вследствие своего удобства и общедоступности, сразу же был взят на вооружение преступными группировками всех направлений.

Понимая, что схема телефонных соединений точно отражает структуру преступного формирования, а сами переговоры позволяют раскрыть содержание криминальной деятельности, правоохранительные органы не могли не воспользоваться этой уникальной возможностью. В результате, подобно Земле в представлениях древних, современная система борьбы с организованной преступностью стоит на трех «китах»: прослушивании те-

лефонных переговоров, анализе добытой информации и судебно-фоноскопической экспертизе.

Прослушиванию телефонных переговоров, накоплению и анализу криминалистически значимой информации нет альтернативы, ибо только этим способом можно распознать за рядом отдельных преступлений хорошо замаскированную, скоординированную и профессионально отлаженную криминальную деятельность организованных преступных групп и сообществ. Значение судебно-фоноскопической экспертизы трудно переоценить, поскольку она почти единственный метод «бесконтактной» идентификации личности, проверки и закрепления следственным путем легализованных оперативных материалов.

Для построения этой системы правоохранительными органами, в особенности МВД и ФСКН России, была проделана большая работа.

В оперативно-розыскной деятельности традиционные сыскные технологии в последние годы заметно уступили место оперативно-техническим мероприятиям, таким как использование систем технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ), снятие информации с технических каналов связи, прослушивание телефонных переговоров, использование средств пеленгации, анализ телефонного трафика, в том числе предусматривающий привязку к базовым станциям, обращение к автоматизированным информационным ресурсам и др.

В УПК РФ четко прописаны процедуры организации контроля и записи переговоров, получения доступа к информации, содержащей охраняемую законом тайну, в том числе – о телефонных соединениях. В этой связи, а также учитывая ограничения, установленные ст. 89 УПК РФ, для обеспечения использования этой информации в доказывании была специально разработана процедура легализации результатов оперативно-розыскных мероприятий.

Задача использования в доказывании информации, перехваченной оперативно-техническими методами, потребовала усиленного развития судебных экспертиз. Так, для обнаружения и изъятия информации, содержащейся в изымаемых у преступников мобильных телефонах и прочих электронных устройствах, активно совершенствуются средства и методы компьютерно-технической экспертизы.

Учитывая транснациональный характер современной преступности, для нужд борьбы с афганским наркотрафиком в течение последних пяти лет ФСКН России разработаны методики идентификации говорящего по голосу и речи на таджикском, узбекском, цыганском и азербайджанском языках. Принимая во внимание, что «базовая» методика фоноскопической экспертизы для русского языка создавалась почти 20 лет, такие темпы развития иначе, чем стремительными, не назовешь.

В целях выявления и объективной проверки информации о структуре преступных сообществ (преступных организаций), уточнения ролей их участников, выявления скрытого смысла в диалогах, иных вопросов,

имеющих важное значение для доказывания состава преступления, предусмотренного ст. 210 УК РФ, ФСКН России была специально разработана методика психолого-лингвистической экспертизы. Ранее подобные исследования проводились филологами русского языка различных педагогических вузов (в Брянске, Владимире и других городах), без какой-либо специальной методики, что резко снижало доказательственное значение конечных результатов.

Получение и анализ информации о телефонных соединениях прочно вошло в следственную практику, став «стандартным», отработанным приемом в работе следователей, независимо от их ведомственной подчиненности[2].

Хотя сменить номер мобильного телефона довольно легко, структура связей между лицами, входящими в преступное сообщество, обладает большой устойчивостью. По этой причине накопление информации о связях членов организованных преступных формирований имеет большое значение в аспекте последующего использования в расследовании. Такая информация должна обязательно накапливаться в соответствующих информационных системах, предусматривающих возможность ее оперативного использования.

В Следственном комитете при МВД России такие сведения аккумулируются в Специализированной территориально распределенной автоматизированной системе органов предварительного следствия и Едином межведомственном банке данных «Невод». В Следственном департаменте ФСКН России, помимо учета следственной информации, на CD-дисках аккумулируются копии самих материалов прослушивания телефонных переговоров и образцов голоса обвиняемых. Это необходимо, поскольку в записях телефонных переговоров наряду с известными членами преступных сообществ фигурирует речь и еще не установленных участников организованного наркобизнеса. В случае если эти лица будут установлены или задержаны, записи ПТП потребуются для доказывания их причастности к ранее расследованным эпизодам преступной деятельности.

Собирание образцов голоса известных наркодельцов также необходимо, поскольку, будучи однажды изобличенными, они редко отказываются от привычного образа жизни. Зачастую, приобретя опыт общения со следствием, они отказываются давать правоохранительным органам образцы своего голоса. А действенного способа принудить их к этому в УПК РФ не предусмотрено. Частная, но острая проблема остается пока нерешенной.

Выявление всех ранее неизвестных эпизодов преступной деятельности обвиняемых является при доказывании признаков организованной наркопреступной деятельности ключевой задачей. Для этого истребуются

[2] См. подробнее: *Жуланов В., Ищенко Е.* Осмотр места происшествия с целью получения информации из электронных баз данных // Законность. 2006. № 6. С. 10–14.

и изучаются уголовные дела, после чего решается вопрос об их соединении в одном производстве. Это сложная и кропотливая работа. Организация «электронного архива» следственной информации позволила бы не только ее облегчить, но и в значительной степени автоматизировать. К сожалению, упомянутые выше системы накопления и анализа следственной информации с данной задачей пока не справляются, что свидетельствует о необходимости их скорейшей модернизации.

Проблема, однако, заключается в том, что основанием для соединения уголовных дел служат не совпадение элементов криминалистической характеристики и не схожий способ совершения преступлений, которые имеют лишь ориентирующее значение, а конкретные судебные доказательства, указывающие на совершение расследуемых преступлений одними и теми же наркодельцами. Поэтому в сведениях по уголовному делу, подлежащему учету в информационной системе, должны быть выделены такие объекты. В первую очередь – лица, проходящие по делу, во-вторых, все, что с ними связано: события (в особенности – преступления), организации, автомашины, номера телефонов, документы и т.д. В-третьих, очень важны корреляционные связи между перечисленными объектами, установление которых и позволяет «выйти» на организованное криминальное наркосообщество.

Полученный модельный образ зарегистрированного уголовного дела будет представлять собой некую семантическую сеть, «узлами» которой станут объекты, а «нитями» – связи между ними. Эта возможность может быть реализована за счет применения специализированных программных продуктов, предназначенных для осуществления приемов следственного анализа. Все они основаны на применении технологии визуального извлечения знаний (Visual Data Mining). Наиболее известны программы таких производителей, как: i2 Ltd., Anacapa Sciences inc., Visual Analytics inc. и др. Они позволяют выявлять сведения, содержащиеся в анализируемых данных в неявном виде, осуществлять поиск скрытых закономерностей и взаимосвязей между объектами, располагают мощным аппаратом визуализации результатов обработки информации.

Ряд вышеуказанных программ специально разработан для следственного анализа телефонных соединений. Использование их возможностей планировалось в составе Специализированной территориально распределенной автоматизированной системы органов предварительного следствия, используемой в следственных подразделениях МВД России в виде типового программного обеспечения интеллектуального анализа (ТИАД)[3]. Однако оно так и не было реализовано по причине его очень высокой стоимости. Было бы целесообразно вернуться к этой идее, возможно – путем разра-

[3] См.: Основные направления комплексной информатизации органов предварительного следствия в системе МВД России на 2002–2006 гг. Методические рекомендации. М., 2002. С. 39–40.

ботки отечественного аналога соответствующего программного обеспечения.

Пожалуй, самой насущной проблемой, стоящей сегодня на пути активного применения в расследовании современных информационных компьютерных технологий, стало отсутствие в следственных органах специальных подразделений, ответственных за эту работу. Множественность ресурсов, условий доступа, технологий обработки и анализа информации указывают на сложность самостоятельного использования их следователем[4].

Давно назрела необходимость создания специальных аналитических отделов при следственных подразделениях для обслуживания собственных информационных ресурсов, обеспечения доступа к ним и использования накапливаемых сведений, осуществления квалифицированного информационного поиска и технологически сложного анализа информации при помощи специального программного обеспечения. Существенную помощь данные подразделения могли бы оказать и в работе по нераскрытым преступлениям прошлых лет, которых с годами становится все больше.

Здесь мог бы очень пригодиться опыт, накопленный в полицейской практике ФРГ, по организации розыскных мероприятий, связанных с целенаправленной компьютерной обработкой различных баз данных в целях поиска сведений о лицах и предметах, представляющих интерес для правоохранительных органов. К их числу относятся розыск в полицейских информационных системах, розыск в иных базах данных, формируемых в интересах уголовного преследования; «сетевой» розыск, связанный с обработкой персонифицированных данных, собранных в ходе проверок людей на границе или на контрольных пунктах; а также растровый розыск.

Сущность растрового метода заключается в том, что он представляет собой автоматизированный поиск неизвестных преступников путем электронной обработки различных информационных массивов персональных данных, собираемых для иных целей, нежели уголовное преследование. В процессе растрового розыска компьютерная обработка широкого круга персональных информационных массивов государственных и негосударственных организаций (учреждений) осуществляется с учетом разрабатываемого правоохранительными органами в поисковых целях так называемого «профиля» (поискового портрета предполагаемого преступника, криминалистической информационной модели последнего), представляющего собой упорядоченный набор поисковых признаков лиц, совершающих данный вид преступлений, в нашем случае – наркодельцов.

В результате обработки баз персональных данных с помощью специальной компьютерной программы из огромного информационного массива выбираются те субъекты, которые соответствуют составленному рас-

[4] См. подробнее: *Жуланов В., Ищенко Е.* Анализ информации из электронных баз данных // Законность. 2007. № 4. С. 26–29.

тру (профилю, портрету), исключая всех тех, кто не совпадает с заданными критериями. По результатам применения растрового метода формируется группа людей, которые соответствуют поисковым признакам потенциального подозреваемого. Их дальнейшая проверка на причастность к организованной преступной деятельности осуществляется с помощью традиционных оперативно-розыскных и следственных действий (электронного наблюдения, задержания, допросов, обысков и др.)[5].

Как было показано выше, массовое восприятие обществом лишь одной технологической новинки в области связи и коммуникации потребовало от правоохранительных органов огромных усилий, чтобы хоть отчасти обуздать возникшие криминальные последствия. Эта работа была проделана, система противодействия выстроена по всей «технологической линии» борьбы с наркопреступностью, создан существенный потенциал для дальнейшего развития.

Однако стремительный прогресс информационных технологий делает это построенное с немалым трудом «здание» чрезвычайно неустойчивым. Современный мобильный телефон становится все более похожим на миникомпьютер. Уже в ближайшем будущем возникнут проблемы, связанные с «освоением» преступным миром целого ряда новых интернет-технологий. Уже сейчас правонарушители, взамен привычной телефонной связи, все активнее пользуются ICQ (централизованная служба мгновенного обмена сообщениями сети Интернет) и Skype[6], что лишает органы правопорядка многих наработанных позиций.

ICQ-сообщения не содержат голоса и устной речи, а потому не пригодны для идентификации средствами судебно-фоноскопической экспертизы. Можно ли по перехваченным сообщениям идентифицировать автора средствами автороведческой экспертизы, – специалистам еще предстоит выяснить.

Skype-сообщения могут содержать и речь, и изображения его участников, однако они передаются в закодированном виде, а «вскрыть» их имеющимися средствами пока невозможно. Данная проблема, по-видимому, имеет наиболее простое законодательное решение. Интернет-провайдеры, предоставляющие эти услуги, должны быть поставлены перед выбором: сотрудничать с правоохранительными органами (разумеется, под судебным контролем), передать коды и сохранять сообщения в течение

[5] См. подробнее: *Сокол В.Ю.* Растровый розыск преступников в Германии: учеб. поС. Краснодар, 2009. С. 6–37.

[6] Skype – бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее шифрованную голосовую связь через Интернет между компьютерами, а также платные услуги для звонков на мобильные и стационарные телефоны. Программа позволяет совершать конференц-звонки, видеозвонки, передачу текстовых сообщений и файлов.

определенного времени, либо вообще отказаться от предоставления этих услуг.

Существенную проблему при установлении отправителей интернет-сообщений создают динамические IP-адреса, присваиваемые пользователю при каждом входе в сеть и являющиеся его идентификатором. Если не обязать провайдеров сохранять эту информацию хотя бы полгода, установить отправителя сообщения будет невозможно, даже если оно было передано со «стационарного» компьютера, не говоря уже о смартфоне.

Статья 186[1] УПК РФ не содержит ответа на вопрос, является ли компьютер в данной ситуации «абонентским устройством» и равнозначен ли номер мобильного телефона динамическому IP-адресу? Если исходить из ст. 53 Федерального закона «О связи», то равнозначен. Но тогда процедура получения этих сведений, в совокупности с отсутствием четких сроков их предоставления провайдером, полностью непригодна в аспекте необходимых темпов расследования преступлений. Эту проблему также необходимо решить в законодательном порядке.

В самом близком будущем можно прогнозировать возрастание криминальной заинтересованности к «закрытым» сегментам Интернета, к программам для анонимной работы в сети, таким, как TOR[7], распределенным хранилищам данных, типа FreeNet, и другим конспиративным возможностям.

Растущая информатизация общества предоставляет всем его членам новые, недоступные ранее возможности. Доступность IT-технологий и широкий спектр предоставляемых ими услуг делают их весьма привлекательными не только для добропорядочных граждан, но и для различных правонарушителей.

Общедоступность и многообразие электронных сервисов в сети Интернет давно оценили торговцы наркотиками. Так, по одному из уголовных дел, расследуемых ныне Следственным управлением Следственного департамента ФСКН России, злоумышленники создали преступное сообщество, которое длительное время занималось распространением наркотических средств группы «JWH», используя возможности сети Интернет. Они располагали собственной оборудованной лабораторией, в которой работал специалист-химик – научный сотрудник местного университета. В лаборатории производились наркотические средства, которые наносились на курительную основу и расфасовывались в удобные для сбыта упаковки.

Наркоторговцы оборудовали целый компьютерный центр, через который осуществляли прием заказов, и распространяли в сети Интернет информацию об ассортименте имеющихся в продаже наркотиков. Оплата «товара» покупателями производилась при помощи электронных платежей, таких как «Яндекс-деньги» и «Webmoney», а также систем мгновен-

[7] См.: *Тимофеев А.* Мама @нархия, папа Интернет // Популярная механика. 2010. № 7 (93). С. 80–83.

ных денежных переводов: «Блиц», «Контакт», «Мигом», «Золотая корона», «Western union».

Доставка наркотиков заказчикам осуществлялась под видом легальных отправлений через компании, предоставляющие почтовые услуги, – СПСР-Экспресс, Почта России, ЕМР и др. К уголовной ответственности по данному делу привлекаются 14 человек, обвиняемых более чем по 250 эпизодам наркопреступной деятельности.

По другому уголовному делу, также расследуемому Следственным управлением ФСКН, преступники разработали и активно эксплуатировали систему «бесконтактного» сбыта наркотиков при помощи электронных платежных терминалов. Изучив места расположения таких терминалов в каком-либо городе, члены преступного сообщества распространяли среди наркозависимых лиц номер контактного телефона, позвонив по которому всегда можно было приобрести наркотики. Позвонившего «диспетчер» отправлял к ближайшему платежному терминалу, где покупатель должен был внести необходимую сумму на «мобильный кошелек». Через Интернет «диспетчер» отслеживал поступление денег в «кошелек», после чего направлял покупателя к месту расположения заранее сделанного тайника – «закладки», в котором тот сам находил оплаченное им количество героина.

Такой способ сбыта наркотиков полностью исключал личный контакт с покупателями и минимизировал риск быть разоблаченными для самих наркодельцов. Полученные деньги переводились на банковские счета, открытые в другом городе на подставных лиц, после чего обналичивались. «Отделения» сети «бесконтактного» сбыта наркотиков действовали на территории Санкт-Петербурга и Ленинградской области, Костромы, Воронежа, Белгорода, Тамбова и других городов России. По делу установлено 43 эпизода преступной деятельности, привлечено к уголовной ответственности 26 человек.

Приведенные примеры далеко не единичны. Организованная наркопреступность осваивает «просторы» глобальной сети значительно быстрее, чем это делают правоохранительные органы.

Одной из сложнейших задач, которые приходится решать следователю при расследовании уголовных дел о преступлениях, совершенных в составе наркопреступных сообществ (преступных организаций), это обеспечение внутренней «подсветки» – т.е. получения доказательственной информации о порядке функционирования этого сообщества, взаимодействия его подразделений и участников в процессе криминальной деятельности «изнутри».

Решение указанной задачи зачастую бывает серьезно затруднено нежеланием обвиняемых давать показания и сотрудничать со следствием, «круговой порукой», столь характерной для организованной наркопреступности, скоординированным противодействием стороны защиты, а то и просто недостатком оперативных материалов, полученных на стадии оперативной разработки.

Правоохранительными органами США специально разработана система ECHELON, позволяющая вести целенаправленный поиск и отслеживать трафик в Интернете, в том числе – в его «закрытых» сегментах. Возможности отечественной СОРМ пока много скромнее.

Решению этой задачи могло бы помочь использование для документирования преступной деятельности на стадии оперативной разработки специального программного обеспечения, позволяющего получать негласный доступ к информации и управлению отдельными устройствами на компьютерах злоумышленников.

Такая программа, разработанная фирмой DigiTask, используется полицией ФРГ для борьбы с наиболее опасными преступлениями. Будучи аналогичной по своей природе вирусу «троянский конь», программа распространяется через Интернет и, «поразив» нужный компьютер, позволяет следить за активностью его пользователя в интернет-браузерах, программах связи типа Skype, электронной почте и чатах, другими словами, обеспечивает производство «электронного обыска». Программа может делать скриншоты (снимки экрана), которые в немецких судах принимаются в качестве доказательств преступной деятельности.

Помимо прослушивания разговоров и слежки за перепиской на компьютере, снабженном такой программой, можно дистанционно включить микрофон или веб-камеру. Таким образом, полиция способна прослушать и увидеть, что происходит в помещении, где находится компьютер. Кроме того, программа позволяет фиксировать все, что печатается на клавиатуре и даже просматривать файлы на жестком диске. Полученные данные, включая записи, сделанные с помощью микрофона и видеокамеры, могут быть сохранены на служебном компьютере, с которого была загружена программа, аналогичная «троянскому коню»[8].

Разработка аналога такой программы и его использование в деле борьбы с компьютеризованной наркопреступностью позволили бы существенно упростить раскрытие и расследование таких преступлений, а также обеспечить суд редкостной возможностью увидеть наркодельцов «за работой».

Использование описываемой программы в нашей стране возможно в рамках оперативно-розыскного мероприятия «снятие информации с технических каналов связи», проводимого под судебным контролем.

Вместе с тем было бы опрометчиво заимствовать что-либо из иностранной практики, не выяснив возможных последствий этого и не рассмотрев претензий, высказываемых в адрес данной технологии на ее родине – в Германии. Необходимо рассмотреть недостатки и выяснить, сможем ли мы избежать их либо проконтролировать в целях исключения возможности наступления негативных последствий, в том числе причинения

[8] *Еремина Д.* Немецкие хакеры взломали правительственную программу для слежки за гражданами // < http://www.lenta.ru/articles/2011/10/11/program/ >

ущерба законным интересам граждан вследствие применения такой технологии.

Первый вопрос, который возникает в связи с предложением использовать вирус для взлома «подозрительного» компьютера у нас в России, не будет ли это мероприятие само по себе преступлением, предусмотренным ст. 273 УК РФ, которая устанавливает уголовную ответственность за создание, использование и распространение вредоносных программ? Безусловно нет, ибо ответ содержится в самом понятии преступления, раскрытом в ч. 1 ст. 14 УК РФ. Поскольку преступлением является лишь общественно опасное деяние, то едва ли им можно посчитать оперативно-техническое мероприятие, имеющее совершенно противоположную направленность: документирование опасной преступной деятельности. Это же можно сказать и по отношению к некоторым другим негласно осуществляемым оперативно-розыскным мероприятиям.

Особенное же возмущение немецкой общественности вызвало то, что программа может не только скачивать данные с пораженных ею компьютеров, но и загружать туда информацию. Таким образом, законность тех или иных доказательств, впоследствии представленных полицией в суд, оказывается сомнительной, поскольку следы собственного пребывания в компьютере программа умеет стирать.

На первый взгляд такие претензии в адрес программы способны серьезно подорвать доверие к полученным при ее помощи судебным доказательствам. Однако при внимательном рассмотрении данный недостаток легко преодолим в рамках следственных технологий, традиционно практикуемых в нашей стране. Результаты прослушивания телефонных переговоров тоже немногого стоят в доказательственном плане, но лишь до той поры, пока принадлежность зафиксированных в них голоса и речи конкретному лицу не будет установлена с помощью судебно-фоноскопической экспертизы.

В рассматриваемом случае полученная с компьютеров правонарушителей информация может быть в ходе расследования перепроверена целым комплексом экспертных исследований. Так, файлы, скриншоты, аудио- и видеозаписи могут быть проверены на предмет аутентичности и возможности создания на исследуемом компьютере путем проведения компьютерно-технической экспертизы. Изображения лиц можно предъявить для опознания, а также подвергнуть криминалистической портретной экспертизе; голоса и речи фигурантов – фоноскопической экспертизе и т.д.

Кроме того, согласно ст. 87 УПК РФ, все доказательства подлежат проверке в своей совокупности путем их сопоставления с другими имеющимися в деле уликами. Для получения дополнительных гарантий, что файлы действительно получены с компьютера подозреваемого (обвиняемого), а не загружены туда самими полицейскими, можно предусмотреть возможность обязательного протоколирования всех действий «троянского коня» путем ведения специального, автоматически формируемого «журнала» – лога.

Независимые программисты указывают, что разработчики немецкой служебной программы не уделили должного внимания ее защите, вследствие чего данные с пораженного компьютера могут попасть в руки киберпреступников. Выяснилось также, что программа хранит собранные сведения на сервере в США, то есть за пределами юрисдикции ФРГ. Анализируя эти недостатки, следует признать их техническими, которых вполне можно избежать при разработке отечественного аналога такой программы.

Более серьезной проблемой может быть названо то обстоятельство, что данная программа распространяется подобно любому вирусу по сети Интернет, а значит, при ее применении сложно избежать поражения других компьютеров. В результате могут оказаться «вскрытыми» и компьютеры людей, не причастных к преступной деятельности, что серьезно нарушит их конституционные права.

Схожая проблема возникает в отечественной практике производства оперативно-розыскного мероприятия «прослушивание телефонных переговоров» (ПТП), когда прослушиваемый на основании судебного решения телефон по какой-либо причине оказывается в руках субъекта, в отношении которого это оперативно-розыскное мероприятие не санкционировалось. Тогда записи разговоров такого лица квалифицируются как «необъектовые», из оперативно-технического в оперативное подразделение (а значит следователю и суду) не передаются, а уничтожаются.

Аналогичный подход может быть применен и в этом случае. Необходимо, однако, предусмотреть техническую возможность уничтожения всех «ошибочно» внедренных вирусов. В противном случае, владельцы случайно «взломанных» компьютеров могут действительно стать жертвой киберпреступников или недобросовестных полицейских.

Еще одной проблемой на пути использования «электронного обыска» для борьбы с организованной наркопреступностью является отсутствие в ФСКН России специальных подразделений, укомплектованных подготовленными специалистами для осуществления оперативно-розыскных мероприятий в глобальной сети с помощью специфических программно-технических средств.

Криминалисты ФРГ также настаивают на усилении оперативного и стратегического анализа и оценки добываемой информации, создании для этих целей в полиции и прокуратуре специальных отделов, пишут о необходимости использования мер телекоммуникационного контроля, а также акустического контроля жилых помещений, предусмотренных § 100a и 110c УПК ФРГ[9].

Конечно, вопрос о применении указанной технологии для осуществления «электронного обыска» в рамках ОРМ «снятие информации с теле-

[9] См. подробнее: *Сокол В.Ю.* Криминалистика в Германии: понятие, система, перспективы: монография. Краснодар, 2010. С. 143–144.

фонных каналов связи» не лишен дискуссионности. Однако нельзя отрицать, что с развитием и распространением широкодоступных Интернет-технологий общественная жизнь, во всех ее проявлениях получила новое измерение. В интересах обеспечения общественной безопасности правоохранительные органы обязаны своевременно «осваивать» это новое информационное киберпространство, а ученые-криминалисты и теоретики оперативно-розыскной деятельности проводить в этом направлении свои научные изыскания. Совместные усилия практиков и теоретиков позволят сократить разрыв между преступным и законным использованием современных компьютерных технологий в сети Интернет.

Вероятно, это потребует совершенствования законодательства, направленного на защиту законных прав и интересов пользователей, дополнения Закона об оперативно-розыскной деятельности, издания необходимых подзаконных нормативных актов, детально регламентирующих проведение оперативно-розыскных мероприятий в компьютерных сетях. Однако на пути применения подобных технологий в нашей стране нет непреодолимых препятствий, поскольку практика борьбы с организованной и технически хорошо вооруженной наркопреступностью требует адекватного ответа на брошенные ею вызовы законности и правопорядку.

Стремительное развитие компьютерных технологий остановить или запретить нельзя. Подобные меры непродуктивны для общества в целом. Поэтому правоохранительные органы должны заранее прогнозировать «побочные эффекты» от внедрения новых информационных технологий и готовиться к их появлению по всем направлениям: в ОРД и криминалистике, в судебной экспертизе и уголовном процессе.

В заключение отметим, что рассмотренные компьютерные технологии могут оказать немалую пользу в борьбе с иными разновидностями организованной преступности, в частности, помочь в отслеживании и пресечении коррупционных связей между организованным криминалитетом и различными эшелонами государственной власти: законодательной, исполнительной, судебной и т.д.

Материал поступил в редакцию 16.11.11.