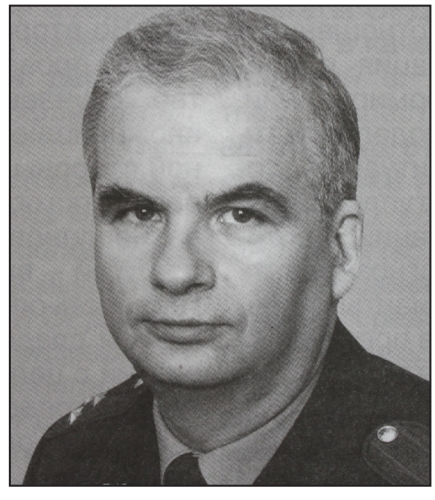
ПРАВОВЫЕ ПРОБЛЕМЫ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ



В. Ф. Луговик,
профессор кафедры оперативно-розыскной деятельности органов внутренних дел Омской академии МВД России, доктор юридических наук, доцент, Заслуженный юрист Российской Федерации

А. Л. Осипенко,
начальник отдела технических средств обучения Омской академии МВД России, кандидат юридических наук, доцент

Оперативно-розыскная деятельность (далее – ОРД) в глобальных компьютерных сетях осуществляется путем проведения оперативно-розыскных мероприятий. Их исчерпывающий перечень дан в ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – закон об ОРД).

На практике проведение оперативно-розыскных мероприятий в глобальных компьютерных сетях принято связывать, прежде всего, со *снятием информации с технических каналов связи*. Несомненно, в силу того, что компьютерные сети относятся к техническим каналам передачи данных, указанное мероприятие будет одним из основных. Однако природа современных глобальных сетей допускает получение оперативных данных не только за счет пассивной регистрации информации, передаваемой по контролируемым каналам связи.

Глобальные сети позволяют применять методы, направленные на активный поиск важных сведений, а в определенных случаях обеспечивать реализацию полученной информации. В целях борьбы с преступностью в глобальных сетях эффективно используется практически весь комплекс оперативно-розыскных мероприятий. Легко заметить, что в том или ином виде с непосредственным использованием глобальных сетей могут выполняться опрос, наведение справок, сбор образцов для сравнительного исследования, наблюдение, контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, оперативный эксперимент. Изучение зарубежного опыта показывает,

что представители спецслужб достаточно эффективно применяют отмеченные способы получения информации.

Представляется, что по мере развития глобальных компьютерных сетей указанный перечень может быть расширен и за счет других оперативно-розыскных мероприятий, определенных законом. Например, появление Интернет-магазинов позволяет уже сейчас осуществлять *проверочные закупки*. Между тем по причине отсутствия единого толкования сущности оперативно-розыскных мероприятий трудно с полной уверенностью сказать, какие из мероприятий, перечисленных в законе об ОРД, могут применяться в глобальных компьютерных сетях. В литературе неоднократно отмечалась необходимость законодательного закрепления норм-дефиниций, посвященных оперативно-розыскным мероприятиям. В рассматриваемом контексте подобные положения закона обеспечили бы более четкое определение мероприятий, допустимых к проведению в глобальных компьютерных сетях. Это важно и с учетом фактического совпадения содержания отдельных оперативно-розыскных мероприятий (таких, например, как «прослушивание телефонных переговоров» и «снятие информации с технических каналов связи»). Даже далекому от техники человеку ясно, что в обычном смысле прослушивание телефонных переговоров является частным случаем снятия информации с технических каналов связи.

Бесспорно, одним из основных среди рассматриваемых мероприятий является *снятие информации с технических каналов связи*. В мировой практике перехват сообщений, передаваемых по техническим каналам связи, применяется в различных целях практически с момента появления самих технических каналов связи. Естественно, глобальные компьютерные сети не могли стать здесь исключением. Прослушивание каналов связи используют как правительственные органы, так и частные структуры, в том числе и криминальные. Во Франции, по сведениям Национальной комиссии по контролю над перехватом сообщений, в год регистрируется до ста тысяч фактов незаконного прослушивания переговоров граждан. По данным ФБР, число запросов на прослушивание сеансов связи в глобальных сетях, поступающих от местных отделений бюро, постоянно растет. Перехват данных в электронных коммуникациях с применением специальных средств проводится и в межнациональном масштабе. Так, в документах Европейского парламента указано, что США производят масштабный мониторинг европейских коммуникаций (в основном, с целью экономического шпионажа). Агентством национальной безопасности США совместно с другими секретными службами разработана и активно применяется глобальная система «Эшелон» (Echelon), предназначенная для перехвата сообщений электронной почты, факсимильной связи и телефонных переговоров. Система действует в интересах правительств США, Англии, Канады, Австралии и Новой Зеландии для борьбы против организованной преступности, терроризма и наркоторговли. По некоторым оценкам, система способна проанализировать до 3 миллиардов сообщений в день. Поиск информации проводится по ключевым словам.

В зависимости от тактических соображений в ходе снятия информации с технических каналов связи может осуществляться пассивный или активный перехват данных. В случае пассивного перехвата выполняется слежение за передаваемыми по каналу связи сообщениями без вмешательства в их поток. Это позволяет раскрывать содержание сообщений, определять объем и частоту передачи, характер передаваемых данных. При активном перехвате над сообщениями уже выполняются определенные действия: они могут быть изменены, уничтожены, задержаны, переупорядочены. Решение тактических задач в определенных случаях может потребовать обеспечения блокировки или задержки всех сообщений конкретному адресату. Такие действия, предпринимаемые в порядке ч. 1 ст. 15 закона об ОРД, могут быть направлены, например, на недопущение получения конкретным адресатом криминальной информации.

Можно заметить, что при данном подходе негласный просмотр электронной корреспонденции на почтовых сетевых серверах и наблюдение за сеансами компьютерной телефонии являются лишь частными формами перечисленных действий, осуществляемых в рамках таких оперативно-розыскных мероприятий, как *контроль почтовых отправлений, телеграфных и иных сообщений* и *прослушивание телефонных переговоров*.

События последних лет убедительно показывают, что обеспечение безопасности граждан и государства в современном мире невозможно без санкционированного в рамках закона контроля со стороны спецслужб информационных потоков криминальных структур и террористиче-

ских организаций. Безусловно, такой контроль не может не вступать в противоречие с интересами обеспечения основных прав и свобод человека. В большинстве государств законы достаточно жестко регламентируют, что соответствующие контрольные действия будут применяться обоснованно и в минимальной степени затронут названные права и свободы. Перехват связи, как правило, допустим только по ограниченному перечню составов преступлений и, за редкими исключениями, проводится после получения судебного решения. В ряде стран предусмотрен особый порядок резервирования данных до получения соответствующего решения суда, допускающего просмотр электронных сообщений. К сожалению, соответствующая процедура до сих пор не нашла отражения в отечественном законодательстве.

Важно подчеркнуть, что даже после получения судебного решения остается проблема выделения из общего потока сообщений информации, связанной с конкретным лицом. Ее сложность усугубляется большим объемом передаваемых данных, подлежащих анализу, и применением изучаемыми лицами средств криптографической защиты сообщений. Нельзя сбрасывать со счетов и возможность подмены сетевого адреса, а также вероятность использования проверяемым субъектом нескольких адресов. В типичной ситуации в многопользовательских системах одно и то же имя может быть доступно разным людям, а один человек может использовать различные имена. Кроме того, с его адреса могут осуществляться сетевые контакты иных лиц, не участвующих в противоправной деятельности.

По законам США, например, в запросе должна быть отражена причина, обусловливающая необходимость перехвата. Указывается, какие иные методы ведения следствия применялись для сбора доказательств, и почему они не дали ожидаемого эффекта. В обязательном порядке представляется информация о любом имевшем место ранее электронном наблюдении в отношении субъекта или сетевого узла. Здесь же перечисляются специфические обстоятельства запрашиваемого перехвата: характеристика совершаемых нарушений, средство передачи данных, точка перехвата сеанса связи, описание типа прерываемых сеансов связи и т.п.

В последние годы при направлении ФБР запроса и выдаче судом постановления, допускающего перехват, принято составлять более подробные документы, чем для прослушивания телефонных переговоров. Такая детализация запроса обусловлена двумя факторами. Во-первых, сложность современных систем коммуникаций требует подробного учета многих параметров сеансов связи. Здесь недостаточно просто указать номер телефона, который будет прослушиваться. В запросе должны найти отражение многочисленные особенности электронных служб, применяемых для передачи сообщений. Во-вторых, нередко в сеансах связи в глобальных сетях пользователи совместно используют различные ресурсы, каналы связи, адреса и т.д. Трудно, а иногда и невозможно выделить из общего потока только те сообщения, в отношении которых имеется решение суда. Возникает необходимость детально описать требования к проведению перехвата, с тем чтобы в минимальной степени нарушить права иных участников сеансов связи.

Достаточно часто принадлежность перехваченного сообщения невозможно определить без его тщательного исследования. По причине значительных объемов передаваемой глобальными сетями информации полный мониторинг электронной почты изучаемых лиц практически недостижим без использования автоматизированных средств анализа. Специализированные программно-аппаратные комплексы перехвата электронных данных позволяют обеспечить и строгое выполнение всех требований решения суда в конкретном случае. В этом отношении любопытен опыт Великобритании и США по созданию систем, отслеживающих и анализирующих электронную почту заданных адресатов[1]. Одним из наиболее известных технических средств подобного рода является применяемый ФБР комплекс Carnivore («Плотоядное животное»). Важно подчеркнуть, что применение Carnivore позволяет обеспечить целостность данных, необходимую для обеспечения доказательственной ценности полученных сообщений. При этом применение Carnivore в США ограничивается несколькими требованиями:

– комплекс применяется только при наличии соответствующего решения суда и только на строго определенный срок;

– установка Carnivore производится только при содействии и технической помощи со стороны представителей поставщика Интернет-сервиса;

– применение Carnivore не допускается в случаях, когда поставщик Интернет-сервиса может самостоятельно долж-

ным образом исполнить решение суда о перехвате.

Последнее означает, что при определенных обстоятельствах провайдеры имеют техническую возможность предоставить правоохранительным органам запрашиваемые данные без применения специальных средств. Например, большинство провайдеров способно самостоятельно скопировать содержимое почтового ящика клиента. Очевидно, в такой ситуации использовать дополнительные специальные средства нецелесообразно.

Опубликованный в Интернет отечественный проект внедрения в глобальных сетях системы оперативно-розыскных мероприятий (СОРМ) вызвал большой резонанс в сетевом сообществе. Проект предусматривал предоставление доступа представителям ФСБ ко всему трафику, проходящему через аппаратуру любого провайдера Интернет. Пользователей сети в первую очередь волнует заложенная в проекте возможность субъектов ОРД без получения специального разрешения осуществлять съем принимаемой и передаваемой информации.

Таким же образом в США провайдеры должны обеспечивать содействие агентам ФБР по Закону о содействии правоохранительным органам (Communications Assistance for Law Enforcement Act, CALEA). В этом документе представляется весьма любопытным положение, в соответствии с которым решение суда, допускающее перехват, обязывает провайдера немедленно снабдить истца всей информацией, средствами и технической помощью, необходимыми для обеспечения перехвата, малозаметно и с минимумом вмешательства в услуги, оказываемые провайдером человеку, связь которого должна быть прервана. Подобное перечисление конкретных действий снимает много проблем, возникающих при оказании операторами связи практической помощи представителям закона.

Современные глобальные компьютерные сети предоставляют оперативному работнику возможность осуществления поиска информации в сетевом компьютере проверяемого лица. Такой поиск, в известном смысле сходный с сетевыми вторжениями хакеров, предполагает применение специального программного обеспечения для дистанционного проникновения в компьютер и последующего обследования содержащихся в нем файлов. Возможно, его следует рассматривать в качестве особого вида оперативно-розыскного мероприятия – *дистанционного обследования помещений, зданий, сооружений, участков местности и транспортных средств*. Хотя основные виды объектов непроцессуального осмотра перечислены в названии данного мероприятия, мы считаем, что в его рамках обследоваться могут и иные объекты преступной деятельности, к которым допустимо относить и сетевые компьютеры.

Тактическое своеобразие удаленного обследования связано с поиском мест проникновения в сетевую компьютерную систему, преодолением установленных защитных средств, сокрытием следов пребывания. Все это требует высокой квалификации и профессионализма исполнителей. На обследуемый компьютер могут скрытно устанавливаться специальные средства (программы регистрации активности пользователя, удаленного управления сетью и т.д.), позволяющие просматривать файлы с электронной корреспонденцией, указатели мест, которые пользователь посещал в Интернет, адресную книгу, отражающую связи проверяемого лица. Нельзя забывать, что изучаемый компьютер может использоваться несколькими людьми, и проведение обследования в таком виде может ущемлять права законопослушных граждан. По этому поводу в рекомендациях ФБР содержится специальное указание о том, что «агент не должен превышать предоставленный уровень доступа и проникать в иные части системы, кроме оговоренных в разрешении»[2].

Дистанционное обследование компьютера практически невозможно без копирования определенных файлов, направленного на их последующее изучение и сравнение с аналогичными образцами, содержащими признаки преступной деятельности. Названные действия можно считать специфическим видом проведения таких традиционных оперативно-розыскных мероприятий, как *сбор образцов для сравнительного исследования* и *исследование предметов и документов*. Закон об ОРД не содержит, но и не ограничивает перечень собираемых оперативным работником образцов, поэтому представляется вполне допустимым отнести к ним и информационные объекты, передаваемые по глобальным сетям, в частности, файлы, содержащие тексты документов, фотоизображения, видео- и аудиофрагменты. Важно отметить, что названные мероприятия могут проводиться не только на сетевых компьютерах проверяемых лиц, но и иных сетевых объектах, например, сайтах Интернет, содержащих образцы порнографической продукции.

При расследовании преступлений не исключена возможность установления контакта между оперативными работниками и определенными лицами с использованием коммуникационных возможностей глобальных сетей (например, электронной почты). При этом в электронном виде может осуществляться *опрос* пользователей сети, которым, вероятно, известны сведения о сетевых преступлениях, причастных к ним лицах, других обстоятельствах, представляющих оперативный интерес (например, слабых местах в защите обслуживаемых объектов и т.д.). Агенты ФБР отмечают, что в некоторых случаях из тактических соображений предпочтение следует отдавать форме проведения опроса, позволяющей оперативному работнику скрывать свои истинные цели и профессиональную принадлежность. При этом для соблюдения конспирации целесообразно выполнить регистрацию специального адреса электронной почты, с которого будет вестись обмен сообщениями с интересующим лицом.

Новые возможности придает использование глобальных сетей и такому мероприятию, как *наведение справок.* В данном случае оно осуществляется путем непосредственного изучения документов, размещенных в сетевых информационных системах и на сайтах, а также направления по сетям запросов в организации, обладающие интересующими сведениями. Контент-анализ содержимого информационных сайтов и сетевых конференций криминальной направленности также позволяет выявлять сведения, представляющие оперативный интерес. В то же время наведение справок не требует получения специальных разрешений, поскольку все подвергающиеся изучению документы находятся в открытом доступе.

Важным мероприятием в плане расширения разведывательных возможностей правоохранительных органов является предусмотренный законом об ОРД в целях выявления тяжких преступлений и лиц, их подготавливающих, совершающих или совершивших, *оперативный эксперимент*.

Интересен опыт западных оперативных служб, применяющих подобное мероприятие не только в отношении конкретных лиц, но и, что особенно значимо, для выявления намерений неизвестных лиц путем создания различных «ловушек» и «приманок». Таковыми в глобальных сетях могут быть, например, файлы с названиями, способными вызвать криминальный интерес, «файлы-улики» со скрытой в них специальной информацией, позволяющей в последующем изобличить преступника при обнаружении у него копий этих файлов. Находят применение сообщения с дезинформацией в местах сетевого общения или в сообщениях электронной почты в случае обнаружения признаков ее перехвата. В практике отечественных правоохранительных органов имеются примеры удачного проведения оперативного эксперимента путем создания фиктивных серверов.

Изучение положительного зарубежного опыта дает возможность рекомендовать и иные методы, успешно показавшие себя в борьбе с преступностью в глобальных сетях. К таковым можно отнести организацию сетевых конференций криминальной направленности, создание контролируемых сетевых объектов, представляющих интерес для преступников (например, электронных магазинов), образование организаций прикрытия (например, фирм, разрабатывающих программное обеспечение или реализующих вычислительную технику). Имитация ложной деятельности в глобальных компьютерных сетях с целью привлечения внимания преступников применяется в особых случаях, поскольку требует существенных затрат различных ресурсов (в основном, финансовых и кадровых). Кроме того, опытный преступник может обнаружить «подвох» и проинформировать об этом сообщников.

Достаточно интересным и показательным примером проведения оперативного эксперимента служат действия агентов ФБР, предпринятые в отношении российских хакеров А. Иванова и В. Горшкова[3]. Последние произвели ряд взломов серверов компаний, расположенных на территории США, похитили конфиденциальные данные и потребовали от руководства компаний выкуп. В июне 2000 г. специалисты ФБР смогли установить личность одного из преступников – Иванова. Было принято решение «заманить» взломщиков в США. Для этого ФБР провело специальную операцию, в ходе которой в Сиэтле была зарегистрирована фиктивная Интернет-компания «Invita»[4]. После того, как хакеры сумели преодолеть ее систему защиты, им было предложено получить хорошо оплачиваемую работу в штате компании в качестве «консультантов по безопасности». Для проведения собеседования российские граждане были приглашены в США, а фирма получила для них визы и оплатила дорогу. В ноябре 2000 г. в офисе компании «Invita» им было предложено продемонстрировать

на практике свои умения и навыки. Подозреваемые выполнили взломы систем защиты перед изображающими персонал компании агентами ФБР. В процессе этого производились сетевые соединения с компьютерами в Челябинске. Манипуляции они осуществляли с рабочих мест, на которые предварительно было установлено специализированное программное обеспечение, регистрирующее производимые действия. В результате у ФБР оказались пароли доступа к персональным компьютерам хакеров. Все происходившее, в том числе и обсуждение с хакерами применяемых методов взлома, записывалось на видеопленку. После завершения «собеседования» оба хакера были задержаны с предъявлением обвинения в мошенничестве нескольких видов. Специалисты ФБР произвели удаленный сетевой обыск находившихся в России компьютеров и получили данные, указывающие на причастность Иванова и Горшкова к противоправной деятельности в отношении американских компаний. В частности, были обнаружены более 56 тыс. номеров кредитных карт, похищенных у американских фирм. В 2002 г. Горшков приговорен американским судом к 3 годам лишения свободы с возмещением убытков в размере 690 тыс. долларов[5].

Следует особо подчеркнуть, что в ходе проведения названной операции агентами ФБР были произведены оперативные действия на компьютерах, находящихся на территории другого государства, что вызвало обоснованные протесты со стороны ФСБ России. Безусловно, в подобной ситуации ФБР следовало обратиться с запросом на проведение обыска к представителям российских правоохранительных органов.

Суммируя сказанное, можно сделать вывод о том, что в настоящее время при осуществлении ОРД непосредственно в глобальных сетях с различным успехом может быть использована большая часть из обозначенных отечественным законом об ОРД оперативно-розыскных мероприятий. Безусловно, при этом полезно учитывать опыт полиции и спецслужб зарубежных стран. Усилия по практической отработке тактических приемов проведения подобных мероприятий будут компенсированы приобретением дополнительных источников оперативной информации, способной не только облегчить раскрытие и расследование конкретных преступлений, но и в определенной степени нормализовать криминогенную обстановку в глобальных компьютерных сетях в целом.

---

[1] См.: *Золотов Е.* СОРМ по-английски // Компьютерра. 2000. № 27. С. 6; *FBI* E-Mail Snooping Device Attacked // Washington Post. 2000. July, 12.

[2] См.: *Federal* guidelines for searching and seizing computers. US Department of Justice, 1999. P. 23.

[3] См.: *Press* Release of U.S. Department of Justice. 2001. August, 16.

[4] Там же. October, 10.

[5] См.: *Баршев В.* С поправкой на бедность // Рос. газета. 2002. 7 окт.