А.Л. Осипенко,
доктор юридических наук,
профессор

НОВОЕ ОПЕРАТИВНО-РОЗЫСКНОЕ МЕРОПРИЯТИЕ «ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»: СОДЕРЖАНИЕ И ОСНОВЫ ОСУЩЕСТВЛЕНИЯ

NEW OPERATIONAL-INVESTIGATIVE ACTION "GETTING COMPUTER-BASEDDATA": CONTENT AND THE BASICS OF IMPLEMENTATION

В статье анализируется содержание нового оперативно-розыскного мероприятия «получение компьютерной информации», прорабатываются основы его практического осуществления, дается классификация источников оперативно значимых компьютерных данных, а также способов доступа к ним.

The article analyzes the content of new operational-investigative activity "getting computer-based data", also explores the basics of its practical implementation, the classification of sources' operative meaningful computer-based data, also ways of access to them.

Обеспечение безопасности граждан и государства невозможно без постоянно осуществляемого правоохранительными органами в рамках оперативно-розыскной деятельности добывания информации о действиях криминальных структур и элементов. В современном мире значительные объемы такой информации циркулируют в сети Интернет, концентрируются в информационных ресурсах и различных технических устройствах в компьютерной форме. В связи с этим в оперативно-розыскной науке и практике ведется активный поиск оптимальных форм и методов сбора компьютерной информации. При этом, как правило, отмечается недостаточная правовая регламентация получения доступа к компьютерным данным в интересах оперативно-розыскной деятельности.

До недавнего времени вариант законодательного закрепления соответствующих действий был предложен лишь в модельном законе «Об оперативно-розыскной деятельности (новая редакция)» (принят на XXVII пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление от 16 ноября 2006 года № 27-6), где соответствующее мероприятие было названо «мониторинг информационно-телекоммуникационных сетей и систем» и определено как «получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам». Полагаем, что такое определение, излишне перегруженное техническими деталями и содержащее технические неточности, не дает достаточно четкого представления о содержании предлагаемого мероприятия. Кроме того, в общепринятом понимании термин «мониторинг» связывается со сбором, анализом и оценкой информации в определенной сфере, деятельностью по наблюдению за соответствующими явлениями, и его использование вряд ли можно признать удачным для обозначения всех тех действий, направленных на получение компьютерной информации, речь о которых пойдет ниже.

Известно, что основным способом собирания оперативно-розыскной информации является осуществление оперативно-розыскных мероприятий (далее — ОРМ), исчерпывающий перечень которых определен в ст. 6 Федерального закона «Об оперативно-розыскной деятельности» (далее — ФЗ об ОРД). Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» дополнил этот перечень мероприятием, названным «получение компьютерной информации». Понятно, что появление ОРМ, учитывающего специфику доступа к информации в современных компьютерных системах, требует детального уяснения сущности и содержания нового мероприятия, проработки основ его практического осуществления.

Для решения этой задачи в первую очередь необходимо разобраться с тем, какое содержание вложено законодателем в ОРМ «получение компьютерной информации». Следует отметить, что выбранное законодателем название нового мероприятия оставляет в этом вопросе неясные моменты. И прежде всего привлекает внимание, что в отличие от названий иных оперативно-розыскных мероприятий оно отражает не способ получения оперативно-розыскной информации, а форму, в которой эта информация представлена.

Практически все предусмотренные ФЗ об ОРД мероприятия направлены на получение оперативно-розыскной информации в той или иной форме (в устной или текстовой, в форме видео- или аудиозаписи, фотоизображения и т.д.). Определенная часть из них допускает получение результатов ОРМ в виде компьютерных файлов (снятие информации с технических каналов связи, наведение справок, сбор образцов для сравнительного исследования, обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.). Почему же законодатель посчитал нужным закрепить получение компьютерной информации в качестве самостоятельного ОРМ?

Очевидно, это решение связано с широчайшей распространенностью компьютерной формы представления оперативно значимой информации и ее специфическими свойствами, обусловливающими особые способы ее получения. Принимая такой подход, анализ содержания нового ОРМ важно начать с уяснения сущности понятия «компьютерная информация».

Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» в ст. 2 дает общее понятие информации — это сведения (сообщения, данные), независимо от формы их представления. Понятие компьютерной информации на уровне законодательства закреплено только в гл. 28 УК РФ, где в примечании 1 к ст. 272 обозначено, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Интересно, что в предыдущей редакции ч. 1 ст. 272 УК РФ компьютерная информация определялась как информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Не отступает от упоминания технических средств и определение, приведенное в Соглашении о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск,01.06.2001), где компьютерная информация обозначена как «информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи». Сравнение показывает, что в новой редакции ст. 272 УК РФ законодатель дал определение компьютерной информации через форму ее представления, а не через перечисление средств ее хранения, обработки и передачи, и сделал это, на наш взгляд, совершенно обоснованно, поскольку спектр таких средств постоянно изменяется и расширяется.

В то же время в официальном отзыве Верховного Суда Российской Федерации от 07.04.2011 № 1/общ-1583 «На проект Федерального закона “О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации”» отмечено, что предложенный термин «электрические сигналы» не вносит достаточной ясности в определение понятия и требует дополнительного пояснения. На это же обращают внимание и отдельные специалисты, отмечая, что развитие способов обработки и хранения компьютерной информации приводит к использованию помимо электрических иных физических явлений, но при этом большинство исследователей сходится в том, что законодательная дефиниция «компьютерной информации» все же вполне адекватна отражаемой ею действительности и оказывает благотворное влияние на правоприменительную деятельность [2, 3].

Итак, под компьютерной информацией следует понимать не какой-то особый вид информации, а специфическую форму ее представления, приспособленную для обработки в компьютерных устройствах, передачи по каналам связи и хранения на специализированных носителях. Уточним, что правильнее здесь было бы говорить даже не об информации, а о данных, которые становятся информацией только при их осмыслении, помещении в определенный контекст [4].

Компьютерная форма позволяет с использованием программного обеспечения эффективно обрабатывать данные, с высочайшими скоростями пересылать их на любые расстояния. Особым свойством, активно используемым преступниками при сокрытии следов противоправных деяний, является обезличенный характер компьютерных данных (отсутствие признаков, прямо указывающих на связь с лицом, их создавшим или подвергшим модификации) и возможность их быстрого полного уничтожения[1].Не менее важна возможность выполнять копирование компьютерных данных при полном совпадении исходных данных и копий, производимых в неограниченном количестве[2].

[1] В специальной литературе в качестве синонимов понятию «компьютерные данные» в рассматриваемом контексте используются термины «электронные данные», «цифровые данные», «виртуальные следы».

[2] Указанное свойство в определенных оперативно-розыскных ситуациях обеспечивает конспирацию проведения ОРМ, поскольку с компьютерных данных, как правило, снимается только копия, а сами данные остаются в неизменном виде, и их владелец не может наблюдать каких-либо признаков того, что произошло копирование информации.

Отметим, что находящиеся в компьютерной форме данные не могут восприниматься человеком непосредственно, поэтому для организации взаимодействия человека с компьютером обязательными являются два противоположных процесса, осуществляемых с помощью специальных программ и устройств ввода-вывода: кодирование (преобразование входной информации в форму, воспринимаемую компьютером) и декодирование (преобразование компьютерных данных в форму, доступную для восприятия человеком) [5].

В качестве компьютеров в настоящее время могут рассматриваться достаточно разнообразные устройства, предназначенные для автоматизированной обработки оцифрованных данных (персональные и сетевые компьютеры, серверы, ноутбуки, сотовые телефоны, смартфоны, планшеты, банкоматы и др.), причем в данном контексте под обработкой можно в широком смысле понимать выполняемые по заданным в программном обеспечении алгоритмам операции по вводу-выводу, передаче, хранению, копированию, модификации, удалению таких данных. Довольно широк и спектр носителей компьютерной информации (встроенные и внешние накопители на жестких магнитных дисках, флэш-карты, оптические диски, CD и DVD диски и др.), на которых она может долговременно храниться и с которых может быть перенесена в компьютер при их подключении к нему. Временно компьютерная информация также может находиться в микросхемах памяти самого компьютера (ОЗУ, ПЗУ, ППЗУ), а также в микросхемах управляемых компьютером периферийных устройств (принтеров, сканеров, факсов и др.). Наконец, она может передаваться между компьютерными устройствами по техническим каналам связи в информационно-телекоммуникационных сетях, подвергаясь при этом обработке (и оставляя определенные следы) в обеспечивающих процесс передачи промежуточных сетевых устройствах (сетевых серверах, маршрутизаторах, концентраторах, модемах и др.).

Отметим, что практически любые данные могут быть переведены в компьютерную форму, которая в настоящее время в основном ассоциируется с цифровой формой представления данных. Интенсивный процесс «оцифровки» данных наблюдается во всех сферах человеческой деятельности, и, по некоторым оценкам, сегодня не оцифровано лишь чуть более 2% доступной информации. Благодаря постоянному снижению стоимости хранения информации в цифровой форме огромные массивы данных могут быть сохранены и использованы для автоматизированной обработки, что открывает в оперативно-розыскной деятельности новые горизонты для информационного поиска [6].

Таким образом, можно считать, что *в техническом плане* получение компьютерной информации может осуществляться:

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 устройств.

Во всех случаях информация может быть получена в виде отдельных текстовых, графических, аудио и видео документов либо выборок по заданным условиям из специализированных баз данных.

С учетом изложенного далее можно уяснить, каково содержание ОРМ «получение компьютерной информации» *с позиций оперативно-розыскной науки и практики*.

Анализ положений ФЗ об ОРД показывает, что законодатель вряд ли связывает его с простейшими формами обращения к компьютерным ресурсам, находящимся у операторов связи или в открытом доступе, либо к устройствам хранения компьютерной информации, полученным в распоряжение субъектов оперативно-розыскной деятельности. Такие действия, осуществляемые, как правило, гласно и не подразумевающие необходимость преодоления определенных препятствий, в большинстве случаев разумно оформлять через иные ОРМ (наведение справок, сбор образцов для сравнительного исследования, проводимое гласно обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.).

Основу ОРМ «получение компьютерной информации», очевидно, 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. Об этом, в частности, свидетельствует и указание в части 4 ст. 6 ФЗ об ОРД на то, что ОРМ, связанные с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности и органов внутренних дел.

Для определения конкретных действий, способных обеспечить получение компьютерной информации в рамках анализируемого ОРМ, целесообразно выделить потенциальные источники оперативно значимых компьютерных данных. Эти источники могут быть разделены на четыре вида, в каждом из которых имеется своя специфика получения компьютерных данных:

1. К *техническим объектам* такого рода могут быть отнесены:

а) потенциально содержащие сведения о разрабатываемых лицах средства вычислительной техники, включая средства сотовой связи и мобильные устройства, обеспечивающие доступ к сетевым ресурсам;

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

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

г) сетевое оборудование, через которое осуществляются коммуникационные акты разрабатываемых лиц.

Следует отметить, что спектр технических источников оперативно значимой информации в ближайшее время будет расширяться и за счет новых видов так называемых «умных вещей», оснащенных микропроцессорами и способных осуществлять обмен данными с телекоммуникационными сетями (навигационные системы автотранспорта, системы «умного дома», бытовые приборы, информационные датчики в местах общественного пользования и т.п.). Смена в современном обществе концепции «Интернет вещей» на «Интернет всего»предполагает подключение к сети практически всех объектов и инфраструктур, обслуживающих интересы как отдельных граждан, так и общества в целом. Понятно, что в потоках данных, формируемых в соответствующих системах, объективно присутствуют значительные объемы информации, представляющей интерес для оперативно-розыскных органов.

2. Получение оперативно значимой компьютерной информации предполагает обследование *информационных объектов сети Интернет*, среди которых выделим:

а) информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется пропаганда криминального образа жизни, вовлекаются в противоправную деятельность новые участники и т.п.);

б) места сетевого общения (закрытые сетевые форумы и чаты, сообщества криминальной направленности в социальных сетях и др.) криминально настроенных лиц и их персональные страницы в социальных сетях.

Оперативно значимая информация на указанных объектах может концентрироваться в виде следов противоправной деятельности, ссылок на материалы, запрещенные к распространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений.

3. Среди источников получения оперативно значимой компьютерной информации особое место занимают *сетевые каналы коммуникации*, задействованные преступниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и т.п. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. При этом важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интернет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegram и др.), причем многие из них предоставляют услуги шифрования передаваемых данных.

4. Оперативно значимая информация может быть получена и из таких источников, как выборки, генерируемые по заданным условиям при анализе сведений из различных *баз данных*, формируемых *в информационных системах* государственных органов и коммерческих структур, в том числе банков и операторов связи.

Итак, с учетом изложенного можно считать, что содержание ОРМ «получение компьютерной информации» связано с применением особых способов доступа к перечисленным выше информационным источникам для достижения указанного в названии мероприятия результата. К таким способам, в частности, могут быть отнесены:

1. Негласное применение специального программного обеспечения и оборудования для скрытного съема данных с компьютерных устройств, потенциально содержащих оперативно значимую информацию, включая негласный дистанционный доступ к компьютерам, имеющим сетевое подключение. Речь здесь, как правило, идет о доступе к информации, которую разрабатываемые лица размещают на закрытых сетевых ресурсах или хранят в своих компьютерных системах и, возможно, не намереваются куда-либо передавать.

2. Оперативно-розыскной мониторинг представляющих оперативный интерес сетевых информационных ресурсов, реализуемый через: автоматизированный поиск ресурсов, содержащих запрещенную к распространению информацию; оперативно-розыскное изучение материалов выявленных ресурсов, связанных с деятельностью преступных сообществ; наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности [7].

3. Негласная установка в компьютерные устройства разрабатываемых лиц специального программного обеспечения, позволяющего фиксировать содержание осуществляемых с этих компьютеров сеансов связи. При этом формирование файлов с информацией о содержании таких сеансов связи, скрытно направляемых на определенный сетевой адрес, происходит на обозначенном компьютере в отличие от ОРМ «снятие информации с технических каналов связи», где информация снимается с каналов связи в процессе ее передачи с использованием предоставляемой оператором связи возможности подключения к указанным каналам.

4. Применение аналитического программного обеспечения для выявления оперативно значимой информации в базах данных различного назначения. Понятно, что в простейших случаях соответствующие выборки могут представляться по запросу органа, осуществляющего оперативно-розыскную деятельность, в рамках ОРМ «наведение справок». Однако есть ситуации, когда субъект ОРД заинтересован в получении от владельца базы данных непосредственного доступа к ней для обнаружения сложных неявных связей между объектами оперативного интереса путем анализа массивов неструктурированных данных из различных источников[3].

Подводя промежуточный итог рассмотрению содержания ОРМ «получение компьютерной информации», следует признать, что, несмотря на отмеченные выше определенные неточности, присущие его названию, все же при разумном нежелании законодателя множить виды ОРМ, направленных на решение одной и той же задачи, охватить все перечисленные действия общим названием было весьма проблематично. С учетом этого полагаем, что предложенное законодателем название ОРМ можно считать вполне приемлемым при том, что в ведомственных нормативных актах будет закреплен развернутый перечень действий, допустимых при его осуществлении на практике, и дана четкая правовая регламентация порядка их реализации.

Далее рассмотрим закрепленные законом условия проведения анализируемого ОРМ. Согласно части второй ст. 8 ФЗ об ОРД оно отнесено к числу ОРМ, ограничивающих конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, и его проведение допускается на основании судебного решения и при наличии информации: 1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; 2) о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; 3) о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Той же статьей допускается возможность осуществлять получение компьютерной информации без судебного решения по основаниям, предусмотренным п. 5 части второй ст. 7 ФЗ об ОРД (связанным с необходимостью на длительной основе организовывать и проводить работу по обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность)при наличии согласия гражданина в письменной форме.

В то же время, очевидно, могут возникать ситуации, когда при доступе к компьютерной информации ограничения конституционных прав не происходит. Так, особого исследования заслуживает вопрос правового регулирования получения информации из массивов персональных данных при условии, что оператор их обработки передает такие массивы субъекту ОРД, предварительно их обезличив (например, заменив конкретные имена, раскрывающие персональные данные, последовательностью условных номеров). Очевидно, что предоставление массивов обезличенных данных не ограничивает конституционные права граждан и, соответственно, может производиться без судебного решения[4].

Следует отметить, что расширение практики осуществления рассматриваемого ОРМ потребует решения целого комплекса организационных и правовых проблем, совершенствования нормативной регламентации вопросов обеспечения прав граждан, а также взаимодействия операторов связи и провайдеров интернет-ресурсов с органами, осуществляющими оперативно-розыскную деятельность, создания реальных правовых условий для организации подключения оперативно-розыскных органов к массивам данных, формируемым в информационных системах государственных органов и коммерческих структур, к системам геопозиционирования, видеонаблюдения и видеофиксации. В частности, в соответствующих нормативных правовых актах должны быть уточнены полномочия полиции по автоматизированному сбору и анализу

[3] Обратим внимание на то, что ст. 2 упомянутого выше Федерального закона от 06.07.2016 № 374-ФЗ дополнила ст. 15 Федерального закона от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности» частью четвертой, закрепившей право федерального органа исполнительной власти в области обеспечения безопасности получать на безвозмездной основе от государственных органов и государственных внебюджетных фондов необходимые для выполнения возложенных на него обязанностей информационные системы и (или) базы данных, в том числе путем получения возможности удаленного доступа к ним.

[4] Действительно, в определенных ситуациях субъекту ОРД достаточно лишь проверить версию о том, действительно ли имело место сочетание каких-либо событий (например, серия звонков на заданный номер с одного и того же абонентского номера и посещение определенного объекта владельцем этого номера в заданном временном промежутке). При подтверждении такой версии для конкретного обезличенного абонента его персональные данные могут быть получены уже в установленном законом порядке после вынесения судебного решения.

разрозненных сведений о поведении граждан, их связях, интересах, финансовых операциях, местонахождении и перемещениях, формированию «электронного досье».

Заслуживают обсуждения и серьезные трудности при получении компьютерной информации, которые могут быть связаны с применением проверяемыми лицами средств криптографической защиты сообщений путем их шифрования. Отдельные государства пытались вводить соответствующие ограничения на использование стойких криптоалгоритмов и применять правовые нормы, регламентирующие доступ представителей правоохранительных органов к зашифрованной информации граждан[5]. Полагаем, что решение этой проблемы следует искать не столько в правовом поле, сколько в адекватном наращивании и технологическом совершенствовании арсенала специальных средств, применяемых оперативными сотрудниками[6]. Разумеется, одновременно возрастает важность правового закрепления допустимости соответствующих процедур и их регламентации в ведомственных нормативных актах.

Завершая рассмотрение, стоит отметить, что в настоящее время дать подробное описание всех особенностей практического осуществления ОРМ «получение компьютерной информации» не представляется возможным, поскольку пока отсутствует нормативное толкование его содержания, а практика применения данного мероприятия еще не наработана в достаточной степени. Между тем потенциал применения этого мероприятия в решении задач оперативно-розыскной деятельности, несомненно, гораздо выше, чем выявление ориентирующих сведений по отдельным делам оперативного учета. Самые серьезные перспективы оно открывает в сочетании с использованием в обработке получаемой компьютерной информации особых технологий анализа так называемых Больших Данных (BigData) [8], позволяющих производить: сбор максимально полной информации об объектах оперативного интереса с формированием «электронного досье» на потенциальных преступников, обнаружением и визуализацией их неявных связей с иными объектами и событиями криминального характера; выявление группировок криминальной направленности и установление их специализации, степени организованности, распределения ролей, причастности фигурантов к тем или иным событиям. Более того, анализ Больших Данных создает реальную технологическую основу использования оперативно-розыскных методов для прогнозирования социально опасных событий и предупреждения преступлений за счет обнаружения «цифровых следов» с заданными свойствами, указывающими на высокую вероятность подготовки либо совершения определенных криминальных действий.

ЛИТЕРАТУРА

1. Горохов Д. Б., Глазкова М. Е. Организация правового мониторинга в системе федеральных органов исполнительной власти // Журнал российского права. — 2008. — № 4. — С. 16—17.

2. Энгельгардт А. А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право: журнал Высшей школы экономики. — 2014. — № 4. — С. 136—145.

3. Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. — 2013. — № 12. — С. 37—40.

4. Мицкевич А. Ф., Суслопаров А. В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. — 2010. — № 2. — С. 206—209.

5. Ефремова М. А. К вопросу о понятии компьютерной информации // Российская юстиция. — 2012. — № 7. — С. 51.

6. Осипенко А. Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. — 2015. — № 2. — С. 13—19.

7. Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы // Научный вестник Омской академии МВД России. — 2010. — №2. — С. 38—43.

8. Овчинский В., Ларина Е. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М., 2014.

[5] В некоторых странах (Великобритания, Франция и др.) действуют нормы, предписывающие подследственным сообщать пароли для доступа к компьютерным данным и иную подобную информацию по требованию представителя следствия, причем в случае отказа назначается дополнительное наказание за создание препятствий осуществлению правосудия.

[6] Так, используемые разрабатываемыми лицами пароли могут фиксироваться в результате установки на целевой компьютер специальных средств, регистрирующих все операции клавиатурного ввода.