УДК 34—343

А.М. Ишин

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Рассмотрены основные направления использования ресурсов сети Интернет в ходе раскрытия и расследования преступлений. Отмечается, что Интернет определяет способы совершения преступлений, специфику следов преступной деятельности, выбор средств и методов, применяемых в процессе раскрытия и расследования преступлений.

This article considers the basic approaches to the use of Internet resources in the detection and investigation of crimes. It is stressed that the Internet affects ways the crime is committed, the features of criminal traces, and the choice of means and methods used in the process of detection and investigation of crimes.

Ключевые слова: Интернет, расследование преступлений.

Key words: Internet, crime investigation.

Использование глобальной сети Интернет во всех сферах жизни современного общества приводит не только к несомненным позитивным результатам, но и к расширению источников социальной опасности, в том числе связанных с явлениями криминального плана. Неуклонно растет число преступлений, совершенных с использованием Интернета, значителен и наносимый ими ущерб. Преступность в Интернете обретает все более опасные формы, получая при этом ярко выраженный транснациональный характер. Происходит изменение мотивации соответствующей противоправной деятельности, активно осваиваются ее новые формы, расширяется география. Отмечается усиление организованности криминальных структур, использующих возможности Интернета в преступной деятельности.

В настоящее время происходит массовое перемещение в глобальную сеть информации, представляющей интерес для правоохранительных органов. При этом интенсификация информационных потоков позволяет рассматривать Интернет в качестве особого инструмента информационного поиска, а не только в качестве технологической информационной системы.

Сегодня в науке сформировались два основных подхода к пониманию Интернета:

а) с позиций информатики анализируются технологические вопросы его функционирования — как информационно-телекоммуникационного средства, обеспечивающего передачу, обработку и хранение информации (технологический подход);

б) с позиций социальных наук Интернет рассматривается как сложный социокультурный феномен, оказывающий влияние на многие

Вестник Балтийского федерального университета им. И. Канта. 2013. Вып. 9. С. 116 – 123.

стороны жизни общества и образующий особую среду реализации определенных видов деятельности и проявления специфических общественных отношений (социальный подход).

В качестве технологической информационно-телекоммуникационной среды Интернет определяет способы совершения преступлений, специфику следов преступной деятельности, выбор технических средств, применяемых в процессе раскрытия и расследования преступлений, методов получения информации в информационных массивах и т.д.

В качестве нового вида социального пространства Интернет накладывает отпечаток на стратегию и тактику раскрытия и расследования преступлений. Возникающая при его использовании социальная среда порождает специфические виды социальных взаимодействий, сложнейшие процессы детерминации преступности, неизвестные ранее образцы криминальных формирований, без учета которых эффективная борьба с преступностью невозможна.

В Интернете преступник способен одновременно осуществлять ряд различных операций в нескольких вычислительных системах, причем возможно совершение дистанционных действий, направленных на информационный объект, находящийся на значительном расстоянии или не имеющий физической привязки к конкретному месту. Определенные операции могут выполняться с мобильных устройств, в то время как их оператор перемещается в физическом пространстве. В подобных случаях можно говорить в некотором смысле о «размывании» физического места совершения преступления, нарушении его пространственной локализации.

Сетевая социальная среда крайне разнородна, и определенная ее часть, разделяющая социально опасные взгляды, может рассматриваться в качестве криминогенной среды. Принадлежащие к ней субъекты объединяются в маргинальные группы. Комфортные условия, которые предоставлены в сетевом пространстве таким негативно настроенным сообществам, приводят к появлению в нем многочисленных зон общения личностей с отклоняющимся поведением. При этом, например, происходит увеличение количества сетевых ресурсов, носящих экстремистскую направленность. Растет число сайтов, принадлежащих организованным преступным формированиям (ОПФ), через которые они не только обмениваются информацией, но и пытаются популяризировать свои идеи и образ жизни. В сетевом пространстве формируется международный рынок детской порнографии как один из самых прибыльных секторов теневой экономики. Широко возможности Интернета используются для распространения информации о местах сбыта наркотических средств, рекомендаций по их изготовлению.

Через глобальную сеть осуществляется торговля оружием, похищенными номерами кредитных карт.

Участились случаи размещения в Интернете видеосъемок реальных сцен насилия (например, садистских избиений случайных прохожих, снятых на камеры мобильных телефонов).

Сетевые информационные ресурсы становятся источником общественно опасных знаний: здесь приводятся описания способов суицида,

получения взрывчатых и отравляющих веществ, пропагандируются разврат, каннибализм и т.п.

Реальную угрозу интересам общества несет и размещение в Интернете вредоносных программ, устройств компьютерного взлома, методических рекомендаций по применению хакерского инструментария, а также продажа запрещенных к обороту специальных технических средств. Сетевые сообщества, размещающие указанную информацию в Интернете, должны попадать под контроль правоохранительных органов.

Преступность в сетевом пространстве создает новые виды криминальных сообществ, формирует уникальную криминальную субкультуру. Она постепенно «врастает» во многие сетевые процессы, видоизменяет их с учетом своих потребностей. В Интернете правоохранительные органы все чаще имеют дело с профессиональными преступниками, характерные черты которых — высокий уровень технической подготовленности, упорство в достижении цели. Нередко указанные субъекты осведомлены о формах и методах органов предварительного следствия, оказывают активное «интеллектуальное» сопротивление раскрытию преступлений. Наиболее заметную специфику среди таких лиц имеют отдельные участники хакерских групп. Хакерское сообщество образует особую криминогенную среду, способную продуцировать значительное число латентных преступлений. Оно имеет сложную организацию и характеризуется специфическими механизмами взаимодействия участников, неизвестными ранее формами организации групповой противоправной деятельности.

Интернет создает условия для структурной оптимизации криминальных формирований. По оценкам ООН, ОПФ все реже представляют собой крупные иерархические организации [1]. Многие хакерские группы организуются на основе сетевого принципа как временный союз для решения конкретной криминальной задачи. При этом в преступных действиях может участвовать широкий круг лиц, находящихся в разных местах.

Совместная противоправная деятельность в такой группе по отдельным моментам может отличаться от обычных форм соучастия. Здесь нередко отсутствует лидер, участники группы лично не знакомы, а координация деятельности осуществляется с использованием сетевых технологий, причем субъекты, обладающие преступной специализацией, могут одновременно участвовать в деятельности нескольких групп, исполняя в каждой схожие функции.

Преступления, совершаемые в сети Интернет, как правило, характеризуются повышенной скрытностью совершения, обеспечиваемой за счет сложности сетевой инфраструктуры и развитых механизмов анонимности. Многие преступления имеют трансграничный характер, при котором преступник, объект преступного посягательства, жертва находятся под юрисдикцией различных государств. Способы совершения преступлений и применяемых специальных средств отличаются нестандартностью, сложностью, многообразием и частым обновлением. При этом реализация сложных сценариев может осуществляться одним человеком при объединении относительно слабых ресурсов отдельных

компьютеров в мощное орудие совершения преступления. К тому же преступники широко обмениваются сведениями о способах совершения преступлений и результатами противоправной деятельности, которые могут использоваться при совершении новых преступлений.

Преступные действия в основном носят дистанционный характер, без физического контакта преступника и жертвы, причем часть таких действий может выполняться в автоматизированном режиме. Применение стандартизированных орудий совершения преступлений (программного обеспечения) нивелирует индивидуальный «почерк» преступников, а использование особых способов сокрытия следов повышает сложность выявления преступления. Важно учитывать, что следы преступных действий в сетевом пространстве распределяются по множеству объектов при отсутствии четко выраженного места совершения преступления.

Еще в большей степени затрудняет выявление преступной деятельности в сети Интернет ее многоэпизодный характер при множественности жертв в случаях, когда каждой из жертв наносится нечувствительный ущерб, но в целом преступник получает существенные преступные доходы (например, при снятии незначительных сумм со счетов владельцев кредитных карт). При этом эпизоды преступления, происходящие в пределах различных юрисдикций, по отдельности могут восприниматься как не связанные друг с другом и не заслуживающие оперативно-разыскного реагирования.

Полагаем, расследование таких преступлений в информационном плане есть процесс устранения информационной неполноты, возникающей при изучении познаваемого преступного деяния. Устраняется она, прежде всего, в ходе поисковой деятельности следователя в рамках уголовного процесса, которая приводит сначала к установлению, а затем к розыску лиц, совершивших преступление.

Основная цель поиска состоит в выявлении или обнаружении объектов, местонахождение которых неизвестно. Различают два основных варианта данной деятельности. Если разыскивается объект, о котором нет никакой информации, а само существование которого лишь предполагается, как предполагаются и какие-либо признаки, по которым объект, возможно, удастся опознать, то имеет место первая разновидность — «поиск». Если разыскивается объект с известными индивидуальными признаками, то налицо другая разновидность, называемая термином «розыск».

Как известно, событие преступления по отношению к познающему его субъекту — это всегда событие прошлого. Но событие преступления непременно отображается во внешней среде либо в форме материально фиксированных следов, либо в форме образов в сознании людей. При этом и то и другое содержит информацию о событии преступления и преступнике, выявление, анализ, оценка и использование которой составляет основу поисковой деятельности следователя. В ней можно выделить две стадии: а) поиск носителей информации о событии преступления; б) обработка, хранение и использование полученных данных в раскрытии и расследовании преступления.

Поиск носителей информации о событии преступления и составляющих его элементах является ключевым моментом в поисковой и ра-

зыскной деятельности следователя. Лишь после обнаружения носителей информации, определения их как источников сведений, относящихся к событию преступления, возможно решение остальных задач расследования — извлечения, передачи, обработки, а также процессуального оформления полученных данных в доказательства.

По нашему мнению, органы предварительного следствия при осуществлении поисковой и разыскной деятельности с помощью сети Интернет могут использовать два вида информации — исходную и розыскную.

Исходная информация включает в себя сведения, полученные следователем в устной форме или в виде документа:

— в результате проведения первоначальных следственных действий;

— из показаний потерпевших, свидетелей;

— в ходе проведения оперативно-разыскных мероприятий органов дознания и оперативных аппаратов;

— на основе сведений, полученных из сайтов Интернета;

— из учреждений и организаций, располагающих информацией в силу своей профессиональной деятельности (аварийно-спасательные службы, медицинские учреждения).

Исходная информация становится основой для проведения поисковой работы следователя. В зависимости от возможности ее использования она может характеризоваться как ориентирующая или доказательственная.

Разыскная информация включает в себя данные, получаемые органами следствия на различных этапах расследования. Под ней мы понимаем сведения, индивидуализирующие объекты розыска (о внешности, особых приметах разыскиваемого, отличительных особенностях похищенных вещей, номере транспортного средства и др.) и позволяющие вести непосредственный розыск.

Как указывает Р.С. Белкин, розыск «есть функция органов дознания и предварительного следствия». Под объектами розыска понимаются такие, которые «находятся вне пределов досягаемости следователя и суда, а доказывание и процессуальная процедура требует реального (физического и психического) взаимодействия с ними и если их местонахождение в настоящий момент не известно» [2, с. 42].

Соблюдение требований уголовно-процессуального закона при получении фактических данных, имеющих значение для дела, и соблюдение при этом порядка, условий и последовательности соответствующих следственных или поисковых действий — основной признак для разграничения доказательственной и ориентирующей информации. Прежде всего, он позволяет отграничивать доказательства от информации, полученной из Интернета.

Наличие в сетевом пространстве криминогенной среды является основанием для проведения поисковой и разыскной деятельности органами предварительного следствия.

Среди криминогенных объектов поисковой и разыскной деятельности органов предварительного следствия можно выделить:

— объекты, требующие наблюдения в связи с повторяющимися попытками преступных посягательств и (или) наличием условий для их совершения (сайты банковских структур, сетевые объекты, обрабаты-

вающие конфиденциальную информацию, сайты социальных сетей, интернет-магазины, интернет-аукционы и т.п.);

— информационные ресурсы, содержащие криминалистически значимую информацию (сайты, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется пропаганда криминального образа жизни и т.п.);

— места сетевого общения криминально настроенных лиц (открытые и закрытые форумы криминальной направленности, чаты и др.).

Важная для раскрытия и расследования преступлений информация концентрируется на сетевых криминогенных объектах в виде:

а) следов противоправной деятельности;

б) сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений;

в) ссылок на сетевые адреса размещения материалов, запрещенных к распространению;

г) сообщений электронной почты, сеансах прямой связи (IP-телефония, ICQ и т.п.), условных сигналов либо зашифрованных сообщений, размещаемых на общедоступных сетевых информационных ресурсах.

Одним из перспективных направлений оперативного поиска в сетевом информационном пространстве стал интернет-мониторинг, который представляет собой комплексную систему наблюдения за состоянием криминальных процессов в сетевой социальной среде, направленную на сбор, обработку и анализ информации о явлениях криминального плана. Основные направления этого мониторинга, способные обеспечить высокую интенсивность поступления криминалистически значимой информации:

а) автоматизированный поиск сетевых информационных ресурсов, содержащих запрещенную к распространению информацию;

б) изучение выявленных сетевых ресурсов, связанных с деятельностью преступных сообществ;

в) наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности.

Поиск по информационным ресурсам Интернета может быть реализован через различного рода поисковые системы (Google, Yandex, Rambler и т.п.), использующие производительные алгоритмы обнаружения информации по заданным реквизитам. В ходе информационного поиска выявляются сайты, связанные с ОПФ, а также сетевые ресурсы, содержащие запрещенную к распространению информацию.

Поисковые серверы могут применяться также для получения дополнительной информации о пользователе или группе пользователей сети. Сведения о разрабатываемых лицах возможно получить в открытом доступе на их личных страницах в социальных сетях (Одноклассники.ру, ВКонтакте.ру) либо в персональных блогах.

Повышение эффективности интернет-мониторинга предполагает применение контент-анализа, который представляет собой формализованный аналитический метод исследования содержания документов в целях выявления и измерения характеристик социальных явлений,

получивших в них отражение. Основными объектами такого анализа могут быть сетевые информационные ресурсы и тексты в местах сетевого общения (социальные сети, блоги, форумы и т.п.) криминальной направленности.

Контент-анализ позволяет установить присутствие в тексте или массивах текстов ключевых слов, зафиксировать смысловые единицы содержания, частоту их употребления, соотношение различных элементов текста. Получаемые количественные характеристики подвергаются статистической обработке. Основная особенность метода контент-анализа состоит в том, что он дает возможность изучать документы в их социальном контексте. Современное программное обеспечение способно производить категоризацию текстов в анализируемых информационных массивах по тематике обсуждаемых вопросов.

Сопоставление и обобщение полученных материалов позволяет установить ряд иных важных обстоятельств: чьи интересы представлены на сайте, имеется ли связь между владельцами сайта и ОПФ.

Более сложной формой получения криминалистически значимой информации в Интернете считается непосредственное наблюдение за закрытыми для общего доступа местами общения криминальной направленности путем осуществления интернет-мониторинга. Он предполагает постоянное изучение сообщений, публикуемых в соответствующих чатах, конференциях, на форумах, и обеспечивает возможность получать сведения о намерениях участников ОПФ, устанавливать их связи между собой, узнавать детали замышляемых деяний, выявлять признанных лидеров, следить за их перемещениями, вести подбор лиц для привлечения к сотрудничеству и т.д.

В этой связи интересен опыт ФБР США, в определенных ситуациях берущего под контроль выявленные хакерские сайты и форумы и получающего при этом ценную информацию (включая контроль интернет-адресов тех, кто часто посещает эти веб-сайты, характер их активности в сетевом общении, сведения о конкретных фактах преступной деятельности) [3, с. 9].

Интернет создает условия для использования новых форм привлечения граждан к содействию в раскрытии и расследовании преступлений. Одним из наиболее простых способов получения информации от граждан в сетевом пространстве может быть создание специализированных сайтов по регистрации сведений, представляющих оперативный интерес. На таких сайтах выделяются страницы, где можно заполнить форму сообщения о совершенных и подготавливаемых преступлениях, о предполагаемых преступниках, их связях и т.п. Передача сведений о противоправной деятельности может осуществляться с сохранением анонимности заявителя. Хотя анонимные сообщения о преступлениях в соответствии с ч. 7 ст. 141 УПК не могут служить поводом для возбуждения уголовного дела, при наличии в них сведений о совершении преступления или приготовлении к совершению преступления их следует рассматривать в качестве оснований для проведения проверочных мероприятий.

Указанные выше возможности сети Интернет определялись в первую очередь инициативой конкретных следователей и оперативных работников. В настоящее время эти возможности рассматриваются правоохранительными органами в приоритетном порядке.

В мае 2013 г. Следственный комитет (СК) РФ объявил тендер на создание системы, которая будет искать в СМИ и Интернете сообщения о преступлениях, а также анализировать реакцию пользователей на них [4]. Предполагаемая система должна осуществлять мониторинг, во-первых, СМИ, во-вторых, блогосферы и соцсетей. Поиск должен осуществляться по 15 тысячам печатных и 8500 интернет-изданий, а также на теле- и радиоканалах и в информагентствах.

Следственный комитет приводит полный перечень соцсетей, на которых следует искать сообщения о готовящихся и совершенных преступлениях. В этот список вошли «ВКонтакте», «Facebook», «Twitter», «Одноклассники», «ЖЖ», «Мой мир», фотосервис «Instagram», видеохостинги «YouTube», «Rutube», «Smotri. com», и даже геосоциальный сервис «Foursquare», основное общение в котором сводится к написанию комментариев по поводу посещаемых кем-то заведений и чужих «чекинов». СК требует находить в соцсетях первоисточники сообщений и вычленять причины, которые привели к тем или иным событиям, к появлению массовых публикаций на криминальные темы.

Использование информационных технологий в ходе раскрытия и расследования преступлений в современных условиях является необходимым условием ее эффективности, имеет ряд существенных особенностей, знание которых необходимо для сотрудников правоохранительных органов.

Список литературы

1. *Эффективные* меры борьбы с транснациональной организованной преступностью // XI Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Бангкок, 2005.

2. *Белкин Р. С.* Очерки криминалистической тактики. Волгоград, 1993.

3. *Newman G. R.* Sting Operations. Problem-Oriented Guides for Police Response Guides. U.S. // Department of Justice. 2007. №6. P. 8.

4. *РИА Новости :* [сайт]. URL: http://digit.ru/state/20130522/401688249.html#ixzz2Wb79v02g

Об авторе

Анатолий Михайлович Ишин — канд. юр. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: ishin50@mail.ru

About the author

Dr Anatoly Ishin, Associate Professor, Immanuel Kant Baltic Federal University, Kaliningrad.

E-mail: ishin50@mail.ru