Академия управления МВД России

Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения)

Сборник статей
Международной
научно-практической конференции

Москва • 2018

Об издании – 1, 2, 3

ISBN 978-5-906942-68-5

Оглавление

УДК 343:004
ББК 67.52
К 82

Одобрено редакционно-издательским советом Академии управления МВД России

К 82 **Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения)** [Электронный ресурс] : сборник статей Международной научно-практической конференции. – Электронные текстовые данные (2,33 Мб). – М. : Академия управления МВД России, 2018. – 1 электр. опт.диск (DVD-R): 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц; ОЗУ 512 Мб; операц. система семейства Windows; AdobeReaderv. 4.0 и выше; дисковод; мышь. – Загл. с титул. экрана.

Сборник сформирован по материалам выступлений на Международной научно-практической конференции «Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения)», которая состоялась 18 мая 2018 г. в Академии управления МВД России на кафедре управления органами расследования преступлений. В сборнике представлены научные статьи ученых и практиков, а также адъюнктов, аспирантов, соискателей и слушателей по вопросам теории и правоприменительной практики. Редакционная коллегия обращает внимание на то, что научные подходы и взгляды, изложенные в представленных статьях, отражают субъективные оценки их авторов.

ISBN 978-5-906942-68-5

Системные требования: процессор Intel с частотой не менее 1,3 ГГц; ОЗУ 512 Мб; операц. система семейства Windows; Adobe Reader v. 4.0 и выше; дисковод; мышь.

Текстовое электронное издание.

Об издании – 1, 2, 3

Оглавление

Электронное издание создано при использовании программного обеспечения:
AdobeInDesign, Adobe Reader.
Объем издания 2,33 Мб.

Дата подписания к использованию: 06.12.2018 г.
Тираж 10 эл. опт. дисков.

Редактор: *Д. В. Алентьев*
Верстка: *А. А. Мельникова*

Федеральное государственное казенное образовательное учреждение высшего образования
«Академия управления МВД России»
125993, г. Москва, ул. З. и А. Космодемьянских, д. 8.
Тел. 8 (499) 745-82-55

e-mail: mvd.akademy@yandex.ru; press_akadem@mvd.gov.ru; https://а.мвд.рф

ISBN 978-5-906942-68-5

Об издании – 1, 2, 3

Оглавление

О типичных формах использования осужденными информационно-телекоммуникационных технологий при совершении пенитенциарных преступлений

А. В. Акчурин,
кандидат юридических наук, доцент

В статье анализируются типичные виды пенитенциарных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Осужденный, расследование пенитенциарных преступлений, исправительное учреждение, мобильная связь, мошенничество, незаконный оборот наркотиков, массовые беспорядки.

Согласно статистическим данным ФСИН России в 2017 г. в исправительных колониях было зарегистрировано 872 преступления, совершенных осужденными (АППГ – 851)[1].

В официальной статистике, к сожалению, не отражается информация о количестве преступлений, совершенных осужденными с использованием информационно-телекоммуникационных технологий[2].

Вместе с тем масштаб противоправного использования таких технологий в преступных целях осужденных достаточно велик[3]. Подтверждением этому могут служить следующие факты и умозаключения.

Во-первых, это подтверждается данными об изъятых средствах связи у осужденных в исправительных колониях: в 2013 г. – 57 012 шт.; в 2014 г. – 62 890 шт.; в 2015 г. – 64 175 шт.; в 2016 г. – 63 287 шт.; в 2017 г. – 57 309 шт.[4] Несмотря на некоторое сокращение показателя изымаемых у осужденных средств связи, их количество, находящееся в неправомерном пользовании, остается весьма вели-

---

[1] Статистические данные ФСИН России: отчеты о состоянии преступности среди лиц, содержащихся в учреждениях уголовно-исполнительной системы. Форма 2-УИС за период 2016–2017 гг.

[2] *Кубанов В. В., Грязева Н. В.* Криминалистика: учебное пособие. Самара, 2016.

[3] *Жарко Н. В., Новикова Л. В.* Субъективные и объективные факторы как особенности расследования пенитенциарных преступлений // Евразийский юридический журнал. 2016. № 8 (99). С. 219–221.

[4] Статистические данные ФСИН России: отчеты о результатах оперативно-служебной деятельности отделов безопасности исправительных колоний, лечебных исправительных учреждений, лечебно-профилактических учреждений и территориальных органов уголовно-исполнительной системы. Форма СБ-1 за период 2013–2017 гг.

ко, что создает необходимые условия для криминальной активности спецконтингента[1]. Во-вторых, подтверждает этот анализ следственной и судебной практики. Одной из самых распространенных категорий преступлений, совершаемых осужденными, отбывающими наказание в исправительных учреждениях, являются действия, связанные с незаконным оборотом наркотических средств и психотропных веществ[2]. По состоянию на конец 2017 г. в общей структуре пенитенциарной преступности доля преступлений, подпадающих под признаки ст. 228 УК РФ, составило 23 %.

Анализ материалов уголовных дел по данным преступлениям показал, что практически все из них содержат в себе сведения о том, как осужденные при осуществлении своих преступных намерений активно использовали средства мобильной связи[3]. Как правило, такая связь использовалась для поиска и установления контактов с поставщиками наркотических средств, связи с сообщниками, согласования места, времени, способа реализации преступных намерений. Характерным является следующий пример. Осужденный К., отбывающий наказание в виде лишения свободы, посредством сотовой связи договорился с неустановленным лицом о продаже наркотического средства, которое это лицо должно было передать ему через гражданина Т. После этого К. посредством сотовой связи попросил Т. оказать ему содействие в незаконном приобретении без цели сбыта наркотического средства, на что последний согласился. Получив от неустановленного лица наркотическое средство гашиш (анашу, смолу каннабиса) в количестве 10,18 г., Т. приехал к основному ограждению исправительного учреждения. В определенный период времени осужденный К., находясь на территории исправительного учреждения, подал гражданину Т. световой сигнал при помощи сотового телефона, после чего последний произвел выстрел в сторону исправительного учреждения из арбалета стрелой, к которой были прикреплены светодиод и наркотическое средство[4].

---

[1] *Шиханов В. А.*Особенности правового регулирования оборота средств мобильной сотовой связи в исправительных учреждениях уголовно-исполнительной системы // Человек: преступление и наказание. 2016. № 2 (93). С. 96–101.

[2] *Егорова Т.И.* Противодействие незаконному обороту наркотиков в местах лишения свободы // Наркоконтроль. 2017. № 1. С. 33–35.

[3] *Морозов Р.М.* Факторы, влияющие на производство расследования уголовных дел о незаконном обороте наркотических средств в исправительных учреждениях // Уголовное наказание в России и за рубежом: проблемы назначения и исполнения (к 10-летию принятия Европейских пенитенциарных правил) / сборник материалов международной научно-практической конференции. Вологда, 2017. С. 109–113.

[4] Уголовное дело № 14325 возбуждено 22.04.2014 ОД МО МВД России «Кирово-Чепецкий».

Довольно часто осужденные используют средства мобильной связи при даче взятки сотрудникам исправительных учреждений, для чего подбирают сообщников, согласовывают отдельные обстоятельства реализации преступных намерений, перечисляют денежные средства на различные счета[1] и т. п. Так, осужденный П., отбывающий наказание в исправительном учреждении, предложил оперуполномоченному оперативного отдела исправительного учреждения И. незаконно пронести на режимную территорию учреждения два мобильных телефона, пообещав взятку в сумме 10 000 руб. за каждый полученный им телефон. Реализуя преступный умысел на получение взятки, И. тайно пронес на режимную территорию исправительного учреждения два мобильных телефона с зарядными устройствами, которые незаконно передал осужденному. После этого, согласно преступной договоренности, посредством предоставляемого «КИВИ Банк» сервиса Visa QIWI Wallet, осужденный, используя средства мобильной связи, осуществил денежный перевод на счет банковской карты, принадлежащей И.[2]

Использование средств мобильной связи позволяет организовывать и координировать преступную деятельность организованных групп с большим количеством соучастников. Так, при помощи средств мобильной связи осужденные способны координировать деятельность соучастников, а использование информационно-коммуникационных возможностей сети Интернет способно сформировать общественное мнение[3], привлечь максимальное внимание правозащитных организаций, а также иных сочувствующих категорий граждан и организаций с целью создания ложного представления о легитимности противоправных действий осужденных[4].

Так, осужденный А., отбывающий наказание в исправительной колонии, организовал массовые беспорядки, сопровождавшиеся насилием, погромами, уничтожением имущества и оказанием вооруженно-

---

[1] *Филиппов М.Н.* Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов // Ведомости уголовно-исполнительной системы. 2015. № 5 (156). С. 26–30.

[2] Приговор Ловозерского районного суда Мурманской области № 1-30/2015 от 14 декабря 2015 г.

[3] *Беляков А.В.* Использование средств массовой информации при подготовке к дезорганизации деятельности учреждений, обеспечивающих изоляцию от общества // Юрист Поволжья. 2008. № 3–4.

[4] *Тищенко Ю. Ю., Масленников Е.Е.* Оперативно-розыскные аспекты пресечения групповых неповиновений осужденных // Групповые неповиновения и массовые беспорядки в учреждениях УИС / материалы круглого стола под общей редакцией ведущего научного сотрудника ФКУ НИИ ФСИН России, доктора экономических наук, профессора С. В. Гарника. М.: НИИ ФСИН России, 2018. С. 392–394.

го сопротивления представителям власти. Реализуя преступный умысел на организацию и участие в массовых беспорядках, он, совместно с другими осужденными, относящими себя к лидерам группировок отрицательной направленности, путем уговоров привлек не менее 1 100 осужденных, содержащихся в исправительной колонии. Кроме того, путем личных встреч и по средствам мобильной связи они вовлекли в массовые беспорядки не менее 100 человек из числа родственников, друзей и знакомых осужденных, давших на это согласие, обязав тех предварительно вооружиться металлическими и деревянными палками, металлическими трубами и прутами, бейсбольными битами, камнями, пластиковыми и стеклянными бутылками, заполненными снегом и льдом, и иными подручными предметами, используемыми в качестве оружия, необходимыми для возможного силового проникновения внутрь указанного исправительного учреждения, а также воспрепятствования спецподразделениям правоохранительных органов в подавлении массовых беспорядков[1].

Вместе с тем самые изобретательные формы использования информационно-телекоммуникационных технологий в преступных целях демонстрируют осужденные при совершении мошеннических действий, так называемое «мобильное мошенничество»[2], которое совершается осужденными различными способами: телефонные звонки (как случайные, так и адресные); знакомство в социальных сетях с представителями противоположного пола; размещение объявлений в средствах массовой информации о купле-продаже либо оказании услуг; смс-рассылка.

Телефонные звонки являются наиболее распространенным способом мошенничества. При этом осужденные практикуют как случайные звонки на стационарные либо мобильные телефоны, так и адресные.

Случайные звонки связаны, как правило, с поиском возможности завести знакомство с представителем противоположного пола и дальнейшим вхождением к нему в доверие и хищением у него денежных средств путем просьбы их перечисления на номер мобильного телефона, банковской карты, иного счета.

Вместе с тем, весьма распространенным являются случайные телефонные звонки с целью сообщения заранее ложной информации о том, что родственник (сын, муж и т. п.) попал в ДТП и необходимо «уладить» данное происшествие с помощью денежных средств.

---

[1] Приговор Челябинского областного суда № 2-39/2014 от 20 августа 2014 г.

[2] *Фомин Ю. С.* Особенности получения информации из систем мобильной связи при расследовании преступлений, совершенных в исправительных учреждениях // Вестник Владимирского юридического института. 2011. № 3. С. 65–67.

Адресные телефонные звонки осужденные склонны совершать, когда они обладают определенной исходной достоверной информацией, на основе которой они сообщают своему собеседнику ложные сведения, приобретающие тем самым правдоподобный характер, что и вводит потерпевших в заблуждение.

Знакомство в социальных сетях с представителями противоположного пола является также весьма распространенным способом реализации преступниками мошеннических действий. Связано это с тем, что благодаря той информации, которая размещается пользователями на своих персональных страницах в социальных сетях, осужденные имеют возможность предварительно подробным образом изучить предполагаемую «жертву» (половозрастные особенности, автобиографические данные, круг интересов, знакомых, коллег и т. п.), что способствует более успешной реализации своих преступных намерений.

Информационно-коммуникационный ресурс сети Интернет осужденные склонны использовать и таким образом, чтобы совершать звонки не самостоятельно, а осуществлять прием звонков от граждан, которые оказываются заинтересованы размещенным объявлением о купле-продаже чего-либо или оказании каких-либо актуальных услуг.

Наименее распространенным способом мобильного мошенничества, по итогам нашего исследования, является смс-рассылка, как правило, с сообщением о крупном выигрыше (дорогого автомобиля, техники и т. п.) и необходимостью внесения «обязательных» платежей.

Однако необходимо заметить, что зачастую уголовные дела по данным смс-рассылкам не возбуждаются или возбуждаются органами предварительного расследования достаточно редко ввиду своей малозначительности. Речь может идти об ущербе, размер которого относительно отдельного гражданина составляет, например, 60 руб., хотя за счет массового характера таких действий общий объем похищенных средств может быть весьма значительным.

Подводя итог, необходимо отметить, что большое количество изымаемых у осужденных телефонных аппаратов мобильной связи, а также анализ следственной и судебной практики позволяют предположить, что совершение осужденными преступлений с использованием информационно-телекоммуникационных технологий – это тенденция современной пенитенциарной преступности. Предварительный анализ состояния преступности в исправительных учреждениях позволяет с уверенностью утверждать, что количество преступлений, совершаемых осужденными с использованием информационно-телекоммуникационных технологий, многократно больше всех регистрируемых официальной статистикой ФСИН России преступлений.

О некоторых аспектах преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации

В. И. Алескеров,
кандидат юридических наук, доцент,
профессор кафедры
(Всероссийский институт повышения
квалификации МВД России)

В работе представлены некоторые аспекты преступлений экстремистской и террористической направленности, совершаемых с использованием сферы телекоммуникаций и компьютерной информации. Дано понятие компьютерной информации и телекоммуникационной сети. Сделан анализ 28 гл. УК Российской Федерации.

Экстремистская и террористическая направленность, компьютерная информация, телекоммуникационная сеть, субъективная особенность личности, беспилотное воздушное судно (БВС), процессорное оборудование, характерологическая особенность психологии личности преступника.

Преступления экстремистской и террористической направленности, совершаемые с использованием сферы телекоммуникаций и компьютерной информации, несут глобальные угрозы и являются весьма опасными как для нашего общества и государства, так и для всего мирового сообщества в целом. Ущерб, наносимый этими видами преступлений, в настоящее время имеет рост в геометрической прогрессии. Проведенный анализ рассматриваемых видов преступлений показывает, что практически каждое крупное преступление террористической и экстремистской направленности совершается с применением телекоммуникационных систем и компьютерной информации. В связи с этим возникает необходимость установления уголовной ответственности за причинение невосполнимого вреда в связи с незаконным использованием телекоммуникаций и компьютерной информации. Так как в настоящее время участились случаи незаконного использования сферы телекоммуникаций и компьютерной информации, возникла потребность установления нововведения в уголовное законодательство и пересмотр в сторону усиления ответственности в связи с несанкционированным исполь-

зованием информации террористической и экстремистской направленности, хранящейся на различных электронных носителях.

Все мировое сообщество бросает огромные силы, разрабатывает новые способы и средства борьбы с такими особо тяжкими преступлениями, как экстремизм и терроризм, приносящие весьма жестокие и порой непоправимые последствия.

К сожалению, до настоящего времени во многих организациях, предприятиях, учреждениях и отраслях производства по сравнению с информацией, зафиксированной на бумажных носителях, сфера телекоммуникаций и компьютерная информация остается наиболее уязвимой.

Анализ положений действующего Уголовного кодекса Российской Федерации позволяет сделать вывод о том, что законодатель в гл. 28 УК Российской Федерации «Преступления в сфере компьютерной информации» дал несколько понятий, ранее не имевших место не только в понятийно-терминологическом аппарате уголовного права, но и в «информационном» законодательстве, так как ранее не было практических наработок и теоретических рекомендаций по раскрытию и расследованию преступлений в этой сфере. В целях своевременного документирования преступной деятельности данного вида преступлений и получения необходимой доказательной базы в отношении лиц, их совершивших, в 2001 г. в структуре МВД России создано специализированное подразделение – Управление «К» БСТМ МВД России, и 6 сентября 2008 г. было организовано ГУПЭ[1] МВД России.

В настоящее время современное мировое сообщество не может представить свою жизнедеятельность без освоения новых достижений в свете быстро развивающихся информационных технологий. Однако не все слои населения ее достижения используют в благих целях, а наоборот, совершают преступления экстремистской и террористической направленности. Преступления экстремистской и террористической направленности с использованием сферы телекоммуникаций и компьютерной информации носят специфичный характер, в настоящее время – это быстро растущие, набирающие оборот новации в системе уголовного права. Так как способы их совершения настолько многогранны и носят изощренный характер, что порой сотрудникам управлений «К» БСТМ МВД России и подразделений ГУПЭ МВД России при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности.

[1] ГУПЭ МВД России. Главное управление по борьбе с экстремизмом и терроризмом.

В целях своевременного получения информации о расположении быстро передвигающихся лагерей экстремистских и террористических группировок и последующего оперативного развертывания плана по изобличению лиц, входящих в преступные группировки, оперативные подразделения правоохранительных органов Российской Федерации внедряют в деятельность по раскрытию данного вида преступлений современные методы.

Одним из способов своевременного получения информации и раскрытия преступлений экстремистской и террористической направленности становится интенсивно развивающийся метод использования многофункциональных комплексов на основе беспилотного воздушного судна (БВС), которые предназначены для оперативного и достоверного получения информации об объектах различного происхождения, проведения инженерной разведки, выявления электронных компонентов мино-взрывных устройств в грунте, а также для оценки результатов деятельности при осуществлении воздушной разведки протяженных участков местности. Такие многофункциональные комплексы позволяют решать следующие задачи.

Ведение фотографической, телевизионной, инфракрасной, радиотехнической, радиолокационной, радиационной, химической разведки с воздуха.

Проведение аэрофотосъемки высокого качества с использованием профессиональной фотоаппаратуры, создание 3 «D» моделей местности и объектов.

Осуществления наблюдения и охраны районов сосредоточения экстремистских и террористических группировок при проведении специальных мероприятий.

Совсем недавно, а именно в начале января 2018 г., международными террористами были использованы так называемые летательные самодельные беспилотники, начиненные боекомплектами с современным процессорным оборудованием, которые получали свое управление на отдаленном расстоянии посредством возможностей радиолокационных и телекоммуникационных сетей с целью совершения на территории Сирии серии террористических актов. Однако благодаря проведению миротворческой миссии по ликвидации экстремистских и террористических организаций на территории Сирии со стороны военно-космических сил и органов внутренних дел Российской Федерации была проведена контроперация по уничтожению данных беспилотников.

Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики методики раскрытия преступлений экстремистской и террористической направлен-

ности, совершаемых в сфере телекоммуникаций и компьютерной информации (компьютерных преступлений), является субъективная особенность личности преступника, которая на начальном этапе раскрытия преступлений характеризуется лишь скудной информацией.

Мы абсолютно согласны с мнением, высказанным Т. В. Ворошиловой, которая предлагает учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре.[1] Иными словами, немаловажное значение в раскрытии любого вида рассматриваемых преступлений играет своевременно полученная информация, раскрывающая характерологическую особенность психологии личности преступника.

Своевременно полученная информация позволяет при более глубоком анализе определить правильную линию поведения оперативных сотрудников подразделений «К» и ГУПЭ МВД России, сузить круг подозреваемых лиц, установить мотив преступления, способ его совершения, а также выдвинуть конкретные версии, отработка которых точно сориентирует и приблизит оперативных сотрудников и следователей к проведению оперативно-розыскных, специальных технических мероприятий и следственных действий, способствующих раскрытию данного вида подготавливаемых и (или) совершаемых преступлений. Это позволит с наименьшей затратой времени выйти на более точное оперативное сопровождение по установлению конкретных лиц, причастных к совершенному или подготавливаемому преступлению, и, как положительный результат, приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств.

Полагаем, что уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю). При закреплении предложенных определений в базовом для этой сферы законодательстве, например в Федеральном законе «Об информации, информационных технологиях и о защите информации», оно позволит, на наш взгляд, существенно сократить ошибки в правоприменении рассматриваемых уголовно-правовых норм[2].

---

[1] *Ворошилова Т. В.* Социальная и психологическая характеристика личности компьютерного преступника. М., 2009. С. 5.

[2] Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2013. № 2 (26). С. 32–37.

Основные направления исследований в области новых информационных технологий, используемых в криминалистике

Д. В. Алымов,
кандидат юридических наук,
доцент кафедры
(Юго-Западный государственный университет)

В. А. Левченкова,
аспирант кафедры
(Юго-Западный государственный университет)

В статье рассмотрены основные направления совершенствования научно-исследовательской деятельности в области использования в криминалистике новых информационных технологий. Особое внимание уделяется системным преобразованиям самой науки криминалистики и отдельных ее разделов с учетом активизации криминальной деятельности и деятельности по раскрытию, расследованию и предупреждению преступлений в пределах специфической формы объективной действительности, именуемой «виртуальным пространством».

Новые информационные технологии в криминалистике, виртуальное пространство, виртуальные следы.

В настоящее время одним из перспективных направлений повышения эффективности работы правоохранительных органов по раскрытию и расследованию преступлений является внедрение в криминалистику новых информационных технологий.

Новые информационные технологии осваивают не только сотрудники правоохранительных органов, но и представители криминальных кругов. С помощью компьютерной техники и информационно-телекоммуникационных систем совершается огромное количество преступлений, механизм которых установить зачастую довольно сложно.

Высокая активность внедрения современных информационно-компьютерных технологий в криминалистическую деятельность и их освоения отдельными преступниками, а также преступными группами и сообществами существенно изменила современные подходы к развитию самой науки криминалистики и отдельных ее разделов. В современной криминалистической науке все чаще обсуж-

дается вопрос о виртуальных последствиях преступного события, а также способах познания закономерностей механизма совершения преступлений с использованием компьютерной техники и информационных технологий.

Традиционные методы познания преступной деятельности на основе метода материалистической диалектики постепенно вытесняются разработками в области исследования специфической формы объективной действительности, именуемой «виртуальным пространством», статус которого криминалистической и уголовно-процессуальной наукой и практикой до сих пор однозначно не определен. Причиной этому, на наш взгляд, является отсутствие системного подхода к изучению особенностей виртуального пространства и процессов, которые в нем проистекают.

В первую очередь следует уделить внимание общетеоретическим и методологическим основам криминалистики, важнейшими элементами которых являются: предмет криминалистики, методы криминалистики, а также система частных криминалистических теорий.

Современные научные подходы к изучению предмета криминалистики сводятся к поиску возможностей его расширения. Однако многие научные труды или отдельные высказывания ученых по данному вопросу ориентированы в основном на включение в предмет криминалистики тех закономерностей, которые не просто расширяют его познавательные границы, но и способствуют искажению служебной роли науки криминалистики как средства борьбы с преступностью.

По нашему мнению, в вопросе о некой «реконструкции» предмета криминалистики следует учитывать современные условия развития и функционирования преступности, использование преступными элементами возможностей виртуальной среды и средств информационно-компьютерной коммуникации для достижения преступного результата. Поэтому все элементы предмета криминалистики должны оставаться традиционными, но их содержание необходимо дополнить отдельными элементами познавательной деятельности, позволяющими системно подойти к решению задач борьбы с преступностью с учетом бурного развития информационно-коммуникационной среды.

Принципиально новый подход к изучению закономерностей предмета криминалистики с учетом развития новых информационных технологий может поспособствовать пересмотру и дополнению системы частных криминалистических теорий.

В связи с этим следует согласиться с мнением Е. Р. Россинской, которая предлагает разработать новую частную криминалистиче-

скую теорию: теорию информационно-компьютерного обеспечения криминалистической деятельности.[1]

По ее мнению, данная частная теория должна объединять криминалистическое исследование компьютерных средств и систем, рассмотрение в криминалистической тактике особенностей тактики и технологии производства следственных действий, направленных на получение криминалистически значимой компьютерной информации, и служить базой для разработки методики расследования компьютерных преступлений.[2]

Анализируя большое количество традиционных учебников и учебных пособий по криминалистике, можно заметить, что вопросам теории информационно-компьютерного обеспечения криминалистической деятельности уделяется крайне мало внимания.

В связи с этим возникает необходимость концептуальных и прикладных исследований в области информационно-компьютерного обеспечения криминалистической деятельности. Ученые-криминалисты должны всячески способствовать созданию принципиально новой научной парадигмы, ориентированной на системное изучение закономерностей криминальной деятельности и деятельности по раскрытию, расследованию и предупреждению преступлений в рассматриваемой области знания.

Изменения, связанные с освоением виртуального пространства, должны затронуть структурные элементы не только общетеоретических и методологических основ криминалистики, но и систему поисково-идентификационной деятельности и трасологической идентификации в криминалистике.

По мнению Е.П. Ищенко, одним из весьма перспективных направлений приложения усилий криминалистов представляется изучение и использование в следственной деятельности электронных следов, оставляемых в различных информационных базах данных средствами мобильной связи, кредитными, дисконтными картами, проездными документами, снабженными магнитным кодом, персональными компьютерами, подключенными к Интернету, электронными товарными бирками, специальными чипами и другими подобными устройствами, ассортимент которых стремительно расширяется. Выявление, фиксация, расшифровка таких следов, становящихся в последние годы массовым явлением, будут способ-

---

[1] *Россинская Е. Р.* К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3–2. С. 110 (109–117).

[2] *Там же.*

ствовать раскрытию и расследованию самых различных, в том числе и компьютерных преступлений, совершаемых в Интернете.[1]

Однако в системе криминалистической техники нет отдельного раздела, посвященного исследованию компьютерной техники и виртуальных следов преступления. А потому на сегодняшний день данная проблема весьма актуальна. Так, «виртуальный след» подразумевает результат отображения реального процесса или же действия компьютерной системы, связанный с тем или иным преступлением, в виде цифрового образа формальной модели этого процесса. В криминалистической науке и практике виртуальные следы рассматриваются двояко. С одной стороны, они стали применяться в расследовании преступлений, но с другой – официально правового оформления не получили, однако это не мешает применять виртуальные следы на практике[2].

Исходя из вышеизложенного, стоит отметить, что перед учеными-криминалистами необходимо поставить вопрос о возможности формирования новой отрасли криминалистической техники или же подотрасли криминалистического учения о следах, связанной с изучением процессов и явлений, происходящих в виртуальной среде. Это позволит существенно повысить эффективность раскрытия и расследования большинства преступлений, совершаемых с использованием компьютерных технологий.

Виртуальные следы являются специфическим видом следов. Их нельзя отнести ни к материальным, ни к идеальным. Учитывая тот факт, что последствия преступного события формируются в специфической среде, то и виртуальным следам следует отвести отдельное место в классификации всех изучаемых следов в криминалистике.

По мнению Ю. В. Гаврилина, виртуальные следы как специфическая форма преобразования компьютерной информации обладают следующими признаками: 1) отражают событие преступления в информационном поле; 2) являются материальными по своей природе, но не отражают пространственную форму следообразующего объекта; 3) являются результатом преобразования компьютерной информации; 4) служат носителями свойств, присущих компьютерной информации; 5) обладают способностью к дублированию, т. е. к копированию на другие электронные носители без изменения их характеристик[3].

---

[1] *Ищенко Е. П.* Криминалистика: главные направления развития. Уголовно-процессуальные и криминалистические чтения: материалы междунар. науч.-практ. интернет-конф. Иркутск, 16–30 апр. 2012. Иркутск: изд-во БГУЭП, 2012. С. 203.

[2] *Агибалов В.Ю.* Виртуальные следы в криминалистике и уголовном процессе. М., 2012. 152 с.

[3] *Гаврилин Ю. В., Шипилов В.В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 2–6.

В криминалистической науке предпринимались попытки выделить отдельные классификационные группы виртуальных следов.

Так, В.П. Леонтьевым предложена следующая классификация виртуальных следов: 1) локальные, расположенные на устройствах преступника или жертвы; 2) сетевые, расположенные на серверах и коммуникационном оборудовании[1].

А.Г. Волеводз предложил классифицировать локальные виртуальные следы в зависимости от носителя, на котором они были обнаружены: 1) следы на винчестере (жестком диске), стримере (магнитной ленте), оптическом диске, дискете; 2) следы в оперативных запоминающих устройствах компьютера; 3) следы в оперативных запоминающих устройствах периферийного оборудования (принтеры, сканеры и т. д.); 4) следы в оперативных запоминающих устройствах компьютерного оборудования связи и сетевого оборудования; 5) следы в проводных, радио-оптических и других электромагнитных системах и сетях связи[2].

Таким образом, криминалистической науке и практике необходимо выработать систему знаний, позволяющих определить понятие, содержание и значение информационно-компьютерного обеспечения криминалистической деятельности. На сегодняшний день такая система знаний до конца не сформирована. Ученым-криминалистам предстоит большая работа по изучению криминальных процессов, возникающих в специфической среде, именуемой «виртуальным пространством», определению понятия и содержания виртуальных следов и их носителей. С течением времени такая система знаний может подвергаться существенным изменениям с учетом совершенствования научно-технических средств, приемов и методов познания виртуального пространства. Однако уже сегодня современная криминалистика перешла на более высокий уровень и способна использовать в своем арсенале самые передовые технологии, позволяющие расширить пределы доказывания. Не исключено, что в скором времени появятся новые отрасли или подотрасли криминалистики, которые будут успешно использоваться в деятельности по раскрытию, расследованию и предупреждению преступлений в киберпространстве.

---

[1] *Леонтьев В.П.* Большая энциклопедия компьютера и Интернета / В.П. Леонтьев. М., 2006. С. 264.

[2] *Волеводз А.Г.* Противодействие компьютерным преступлениям / А.Г. Волеводз. М., 2002. С. 159–160.

Методико-криминалистические проблемы расследования порно-сексуальных преступлений, совершенных с использованием информационно-телекоммуникационных технологий

О. Ю. Антонов,
декан факультета,
доктор юридических наук, доцент
(Московская академия Следственного
комитета Российской Федерации)

В статье рассматриваются проблемы методико-криминалистического обеспечения взаимосвязанных половых преступлений, а также изготовления и распространения порнографических материалов, совершенных с использованием информационно-телекоммуникационных технологий. Описаны взаимосвязи четырех типов порно-сексуальной преступной деятельности. Предложены пути решения проблем, возникающих в ходе ее расследования, в том числе путем создания нового криминалистического учета.

Сексуальные преступления, киберпреступления, Интернет, организация расследования, криминалистический учет.

В условиях развития информационного общества расширяются возможности его использования в преступной деятельности. Увеличение числа пользователей и отсутствие физических границ информационно-телекоммуникационных сетей позволяет преступникам осуществлять негативное воздействие в отношении лиц, проживающих в других регионах земного шара. В качестве потерпевших достаточно часто выступает такая незащищенная часть населения, как несовершеннолетние.

По мнению В. В. Соловьева, снижение возраста пользователей социальных сетей, относительная анонимность внутрисетевой деятельности, скорость распространения информации и возможности подбора целевой аудитории позволили значительному количеству лиц с нарушением сексуального предпочтения в форме педофилии стать «ближе» к несовершеннолетним в виртуальном пространстве[1].

[1] *Соловьев В. С.* Использование социального сегмента сети Интернет для совершения посягательств на половую неприкосновенность несовершеннолетних // Вестник Московского университета МВД России. 2017. № 3. С. 192.

Так, Н.С. Бельская полагает, что одним из наиболее серьезных рисков для детей и подростков в Интернете является «кибергруминг», или «онлайн-груминг» (cybergrooming/onlinegrooming), который определяется как тактический подход взрослого человека к несовершеннолетнему с целью подготовки к сексуальным отношениям и, в конечном итоге, к эксплуатации. В качестве инструмента «грумминга» выступает «секстинг» как обозначение вида виртуального секса – процесса, во время которого онлайн-коммуниканты соединяются вместе для обмена электронными текстовыми сообщениями – «секстами» с вложением визуальных материалов (личных фотографий и видео) на сексуальную тему при помощи технологий дистанционной связи и мгновенного месседжинга[1].

Например, Т., используя способ электронной передачи данных посредством сети Интернет, а именно социальную сеть «Вконтакте», неоднократно направлял текстовые и графические сообщения несовершеннолетней Ш., содержащие картину совершения с последней полового акта и требования вступить с ним в половую связь, а также угрозы применения насилия в случае отказа подчиниться его требованиям. Неоднократно получив отказ Ш. вступать с ним в половую связь, Т. дважды насильно привез Ш. к себе домой и первоначально совершил в отношении нее насильственные действия сексуального характера, а в последующем – изнасилование[2].

Указанные действия подпадают под признаки преступлений, предусмотренных ст. ст. 131–135, 137, 242, 242.1, 242.2, 240.1, 241 Уголовного кодекса РФ, поскольку связаны с совершением с помощью информационно-телекоммуникационных сетей половых преступлений и/или с изготовлением и распространением порнографических материалов, в том числе носящих характер сведений о частной жизни потерпевших. Их можно объединить в группу с условным названием «порно-сексуальные киберпреступления», выделив ее четыре основных типа: корыстно-организованная, корыстно-профессиональная, сексуально-индивидуальная, сексуально-преступная деятельность, которые имеют свои особенности как осуществления, так и воспроизводства.

---

[1] *Бельская Н.С.* Речевой жанр секстинга в судебной лингвистической экспертизе интернет-коммуникации при расследовании преступлений против половой неприкосновенности и половой свободы личности // Вестник Кемеровского государственного университета. 2015. № 1 (61). Т. 2. С. 170.

[2] Обвинительное заключение по уголовному делу № 4716213-2014. следственного отдела по Калининскому району г. Челябинска СУ СК России по Челябинской области. По материалам Московской академии Следственного комитета Российской Федерации.

Корыстно-организованный тип осуществляется организованными преступными группами, занимающимися изготовлением порнографических материалов с привлечением большого числа участников (моделей), в том числе несовершеннолетних, в целях последующего распространения на платной основе через интернет-ресурсы, как правило, размещенные (зарегистрированные) за рубежом либо путем рассылки конкретным клиентам.

Корыстно-профессиональный тип является, как правило, производным от первого вида, поскольку совершается одним лицом либо небольшой группой лиц по предварительному сговору и осуществляется путем скачивания порнографических материалов, размещенных на различных информационных ресурсах, и их рассылки клиентам за определенную плату.

Результатом первых двух видов преступной деятельности может быть возникновение ее третьего вида – сексуально-индивидуального, включающего поиск, скачивание, распространение и получение путем обмена в электронном виде порнографических материалов лицом, удовлетворяющим свои индивидуальные сексуальные потребности путем просмотра порнографических изображений, в том числе с участием несовершеннолетних.

Третий тип может трансформироваться в четвертый – сексуально-преступный, который осуществляется одиночками, в том числе страдающими психическими расстройствами на сексуальной почве и использующими порнографию в качестве способа развращения несовершеннолетних с последующим совершением в отношении них преступлений против половой неприкосновенности и половой свободы личности как виртуальным способом, так и непосредственно путем личного контакта («кибергруминг»). Последние действия могут совершаться и без направления потерпевшим порнографии.

В целях изучения взаимосвязей данной группы преступлений в рамках единой преступной деятельности можно использовать подход В.Ф. Ермоловича, использующего в качестве основы криминалистических характеристик отдельных видов преступлений их криминалистические структуры, которые открывают хорошие перспективы и возможности для того, чтобы перейти на более высокие уровни обобщения сведений о преступлении, выявлении связей и зависимостей между его элементами, оставляемыми ими следами и, естественно, для дачи более широкого круга конструктивных рекомендаций[1]. Представляется, что необходимо определять

[1] См.: *Ермолович В.Ф.* Перспективы развития криминалистической характеристики преступлений // Проблемы управления. 2012. № 3. С. 56.

не только криминалистическую структуру преступлений определенного вида, но и возможные взаимосвязи среди структур сопряженных преступлений в динамике возникновения и развития преступной деятельности, включающей в себя несколько видов взаимосвязанных преступлений.

Такие взаимосвязи можно проследить следующим образом. Субъекты организованно-корыстной преступной деятельности изготавливают порнографические материалы, распространяя их субъектам корыстно-профессиональной, сексуально-индивидуальной и/или сексуально-преступной деятельности. Субъекты второго типа также могут распространять данные материалы субъектам третьей и четвертой категории. Последние две группы лиц могут обмениваться ими между собой, делиться преступным опытом либо размещать порнографию на личных страницах в социальных сетях. Лица, входящие в четвертую категорию, могут направлять порнографические материалы выбранным потенциальным жертвам сексуальных преступлений, а также получать их обнаженные фотографии (видеозаписи) либо фиксировать с помощью фото – и/или видеосъемки свои преступные действия сексуальной направленности, то есть становиться не только распространителями, но и изготовителями порнографии, а полученные или изготовленные порнографические материалы могут распространять всем категориям субъектов рассматриваемого вида преступной деятельности. Аналогичного мнения придерживаются И. А. Семенцова и А. И. Фоменко, считающие, что при помощи сети Интернет педофилы получают поддержку от лиц с подобными расстройствами, они обмениваются порнографическими фотографиями детей, делятся своим криминальным опытом[1].

В связи с этим, после выявления и пресечения конкретного преступления, связанного с изготовлением и распространением порнографических материалов и/или сексуальной направленности, по нашему мнению, следует выполнить комплекс следственных действий и оперативно-разыскных мероприятий в целях установления, во-первых, всех эпизодов преступной деятельности в отношении всех возможных потерпевших, во-вторых, контактов подозреваемого (обвиняемого), которые занимаются изготовлением и распространением порнографических материалов либо совершением сексуальных преступлений путем знакомства с жертвами в социаль-

[1] *Семенцова И. А., Фоменко А.И.* Актуальные вопросы предупреждения преступлений, совершаемых лицами с расстройством сексуального предпочтения (педофилией) посредством сети Интернет // Теория и практика общественного развития. 2015. № 10. С. 91.

ных сетях, в-третьих, посещаемых им интернет-ресурсов, распространяющих порнографию.

Например, сотрудникам МВД России удалось выявить интернет-форум, который использовался педофилами для обмена фотографиями и видео. Помимо общедоступной части существовала и закрытая секция, предназначенная для общения изготовителей детской порнографии, для доступа к которой требовалось регулярно предоставлять собственноручно отснятые порноматериалы с участием несовершеннолетних. В закрытом сообществе состояло 20 педофилов со всей страны[1].

Если следовать предложенным криминалистическим рекомендациям, то в следственной практике возникает организационная проблема возбуждения уголовных дел и расследования дополнительных эпизодов преступной деятельности, совершенных одним лицом в отношении нескольких потерпевших, проживающих в различных регионах России. Дополнительно может возникнуть обратная практика одновременного возбуждения и параллельного расследования следственными органами Следственного комитета Российской Федерации по субъектам РФ уголовных дел в отношении потерпевших, проживающих на их территории, при совершении указанных преступлений одним и тем же лицом.

В первом случае можно рекомендовать следователю, возбудившему первоначальное уголовное дело, в случае выявления потерпевших, проживающих в другом регионе, выделять материалы и направлять их по их месту жительства в целях возбуждения нового уголовного дела и проведения необходимых следственных действий с данным потерпевшим. Впоследствии вышестоящий руководитель следственного органа (Председатель Следственного комитета Российской Федерации или его заместитель) вправе определить подследственность по месту совершения большинства эпизодов или месту жительства установленного обвиняемого (в случае его проживания на территории России) либо поручить расследование Главному следственному управлению Следственного комитета Российской Федерации.

Во втором случае в целях своевременного выявления серийных преступлений можно ввести учет ip, id-адресов (в том числе зарегистрированных за границей), используемых при совершении преступлений. В связи с наличием программного обеспечения, моделирующего (маскирующего) указанные адреса, а также в целях опера-

[1] См.: В России ликвидировано сообщество изготовителей детского порно // URL: http://gosindex.ru/news/novosti/detskoe-porno (дата обращения: 08.12.2016).

тивности выявления серийных преступлений ведение такого учета можно поручить подразделению МВД России, осуществляющему оперативно-разыскую деятельность по борьбе с преступлениями, совершенными в сфере телекоммуникаций и компьютерной информации.

Дополнительно в целях выявления серийных преступлений можно предложить введение криминалистического учета порнографических материалов с указанием их частных признаков в целях определения единого источника изготовления (происхождения). В рамках такого учета возможно решение следующих задач: идентификация материала в целом (например, видеоролика), отдельных его элементов (например, изображений) либо участвующих лиц (по признакам внешности или голосу), а также способа его изготовления или создания информационного ресурса в сети Интернет, на котором он был размещен, либо оборудования, использовавшегося для его создания или размещения, либо автора использованного в нем печатного текста достаточного объема.

По результатам решения данных задач можно решать вопрос о соединении уголовных дел по фактам изготовления и распространения порнографических материалов, совершенных одним лицом либо преступной группой, что позволит как пресечь их преступную деятельность, так и снять с учета факты распространения одними лицами однородных порнографических материалов[1].

Таким образом, изучение практики совершения и расследования порно-сексуальных киберпреступлений ставит новые организационные задачи, требующие своего методико-криминалистического обеспечения.

---

[1] В части учета преступлений изготовление и распространение порнографических материалов сходно с изготовлением и сбытом поддельных денежных средств, где все факты сбыта одним лицом одной серии поддельных денег, изготовленных одним способом, охватываются единым умыслом и при соединении уголовных дел на учете остается одно преступление. Для установления факта изготовления нескольких денежных купюр, сбытых в разных местах, в том числе в разных регионах России, достаточно давно и успешно используется соответствующий экспертно-криминалистический учет, ведущийся на федеральном уровне.

Актуальные проблемы расследования преступлений в сфере компьютерной информации

И. А. Архипова,
заместитель начальника кафедры,
кандидат юридических наук, доцент
(Московский университет МВД России
им. В. Я. Кикотя)

В статье рассматриваются особенности расследования компьютерных преступлений, а также тактика производства отдельных следственных действий при расследовании указанных преступлений.

Расследование преступлений, компьютерные преступления, тактика производства отдельных следственных действий.

В настоящее время криминализация сферы оборота компьютерной информации набирает высокие темпы. Массовая компьютеризация привела к развитию рынка компьютеров и программного обеспечения, повышению профессиональной подготовки пользователей, увеличению потребностей организаций в совершенствовании технологий обработки данных, значительно расширила сферу применения компьютерной техники, которая все чаще подключаются к сетям широкого доступа. Активно внедряется автоматизированная обработка бухгалтерской и иной производственной документации. Информация, содержащаяся в компьютере, зачастую вообще не хранится на бумаге. Компьютер стал практически обязательным элементом рабочего стола не только руководителей, но и рядовых сотрудников. Указанные обстоятельства не могли не отразиться на криминальной сфере общественной жизни. Преступления, совершенные с использованием компьютерных технологий, в последнее время стали одними из наиболее распространенных.

При расследовании указанной категории преступлений можно выделить следующие типичные следственные ситуации: 1) преступление, связанное с движением компьютерной информации, произошло в условиях очевидности, его характер и обстоятельства известны (например, какой вирус и каким способом введен в компьютерную сеть) и выявлены потерпевшим собственными силами, преступник известен и задержан; 2) способ совершения преступления известен, но механизм преступления в полном объеме неясен (например, произошел несанкционированный доступ к файлам

законного пользователя через Интернет, через слабые места в защите компьютерной системы); 3) налицо только преступный результат, например дезорганизация компьютерной сети банка, механизм преступления и преступник неизвестны.

В первом случае необходимо установить, имелась ли причинно-следственная связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями (сбоями в работе, занесением компьютерного вируса и пр.), определить размеры ущерба. Во втором – первоочередной задачей, наряду с указанными выше, является розыск и задержание преступника. И наконец, в наименее благоприятной (третьей) ситуации необходимо установить механизм преступления.

Остановимся подробнее на особенностях тактики отдельных следственных действий, в ходе которых производится обнаружение, фиксация, изъятие компьютерной информации, а именно: следственного осмотра (предметов, документов), обыска (в том числе личного, в помещении и на местности), выемки (предметов, документов, почтово-телеграфной корреспонденции). При производстве указанных следственных действий необходимо тактически правильно производить поиск информации в компьютере, что позволит избежать ее уничтожения или повреждения; зафиксировать и изъять компьютерную информацию в соответствии с процессуальными нормами. Современное развитие информационных технологий позволяет хранить огромные массивы информации в незначительных по размеру устройствах.

При подготовке к осмотру, обыску или выемке следователь решает вопрос о необходимости изъятия компьютерной информации, при этом важно получить достоверные данные о виде и конфигурации используемой компьютерной техники; о том, подключена ли она к локальной сети или Интернету; о наличии службы информационной безопасности и защиты от несанкционированного доступа; системе электропитания помещений, где установлена техника; квалификации пользователей. Владение такой информацией облегчит следователю доступ к хранящейся в компьютере информации и максимально повысит ее доказательственную базу.

Часто решающее значение имеет внезапность обыска (неотложность осмотра), поскольку компьютерную информацию можно быстро уничтожить. Если получены сведения о том, что компьютеры организованы в локальную сеть, следует заранее установить местонахождение всех средств компьютерной техники, подключенных к этой сети, и организовать групповой обыск одновременно во всех помещениях, где установлены компьютеры. Перед началом

обыска (осмотра) принимаются меры, которые предотвратят возможное повреждение или уничтожение информации. Для этого следует обеспечить контроль за бесперебойным электроснабжением в момент осмотра, удалить всех посторонних лиц с территории, на которой производится осмотр или обыск, прекратить дальнейший доступ; принять меры к тому, чтобы оставшиеся лица не имели возможности прикасаться к компьютерной технике и к источникам электропитания. Если на объекте находятся легковоспламеняющиеся, едкие вещества, посторонние источники электромагнитного излучения и другие предметы и аппаратура, способные привести к аварии, их необходимо эвакуировать. Осмотр или обыск целесообразно производить с участием специалиста в области информационных технологий.

Не следует ограничиваться поиском информации только в компьютере; необходимо внимательно осмотреть имеющуюся документацию, поэтому любые обнаруженные носители информации должны быть изъяты и изучены.

Только после перечисленных подготовительных мер следует приступать к рабочему этапу следственного действия. Изучение практики показывает: несоблюдение элементарных правил ведет к тому, что деятельность следователя по сбору компьютерной информации не достигает своей цели. Тактика поиска компьютерной информации должна выбираться исходя из, во-первых, степени защищенности данных, во-вторых – функционального состояния компьютера и периферийных устройств на момент производства следственного действия.

О высокой степени защищенности компьютера может свидетельствовать наличие специальных систем защиты информации от несанкционированного доступа и (или) сертифицированных средств защиты; постоянная охрана территории и здания, где размещается компьютерная система, с помощью технических средств и специального персонала, использование строгого пропускного режима, специальное оборудование помещений; наличие администратора (службы) защиты информации. Низкая степень защищенности определяется наличием простого алгоритма ограничения доступа (например, данные защищены только паролем), получением достоверных данных о его преодолении, при этом нет необходимости применять специальные средства доступа к данным.

Деятельность следователя по преодолению защиты компьютера от несанкционированного доступа – одна из самых ответственных. Именно при некорректном обращении защищенные данные могут быть самоуничтожены, искажены, спрятаны и т. д. с помощью спе-

циальных программ. Чтобы этого не произошло, при подготовке к проведению следственного действия необходимо как можно более точно и полно определить степень защищенности компьютера, средства защиты, пароли, ключевые слова и т. д.

С одной стороны, по общему мнению специалистов в области программирования, на сегодняшний день нет программно-технических средств, способных стопроцентно гарантировать защиту. Отсюда следует, что, в принципе, возможно преодолеть любую преграду при поиске информации. С другой стороны, существующие средства защиты настолько разнообразны, используют различные алгоритмы и принципы построения защиты, что для их преодоления может понадобиться немало времени. В среде хакеров именно преодоление защиты от несанкционированного доступа является одним из высших подтверждений мастерства.

При первоначальных допросах свидетелей и потерпевших необходимо выяснить назначение и функции компьютерной системы, кто имел доступ к ней и в помещения, где располагалась компьютерная техника, не появлялись ли там посторонние лица, какие средства защиты использовались. Если часть информации была закрытой, то кто санкционировал доступ к ней и кто реально был допущен. Какой вред (имущественный, неимущественный) причинен преступлением и имеются ли способы устранить или уменьшить вред, причиненный несанкционированным проникновением в систему.

При производстве допросов подозреваемых и обвиняемых необходимо учитывать данные криминалистической характеристики личности предполагаемого преступника. Важной является подготовка к допросу, в процессе которой необходимо постараться хотя бы условно выбрать, к какой группе относится подозреваемый или обвиняемый, и на этом основывать тактику допроса. При первоначальном допросе необходимо, побуждая лицо к деятельному раскаянию, выяснить, какие изменения в работу компьютерных систем были внесены, какие вирусы использовались.

Выше уже отмечалось большое значение, которое имеет участие специалиста в собирании доказательственной информации по делам данной категории. Но наиболее важен ее дальнейший анализ, исследование доказательств в ходе экспертных исследований. Основной род экспертиз в данном случае – компьютерно-технические. В соответствии с их задачами и спецификой объектов исследования в настоящее время, в рамках этого рода экспертиз, можно выделить два вида: техническая экспертиза компьютеров и их комплектующих, которая проводится в целях изучения конструк-

тивных особенностей и состояния компьютера, его периферийных устройств, носителей и т. д., компьютерных сетей, а также причин возникновения сбоев в работе и экспертиза данных и программного обеспечения, осуществляемая в целях изучения информации, хранящейся в компьютере и носителях.

По делам данной категории могут также назначаться судебно-экономические экспертизы, в частности финансово-экономические и бухгалтерские, например, когда преступления в сфере движения компьютерной информации связаны с преступлениями в кредитно-финансовой сфере. Весьма распространены технико-криминалистические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов и фальшивых денежных банкнот.

Экспертные системы в интеллектуальном обеспечении уголовного процесса и криминалистики

А. Ю. Афанасьев,
преподаватель кафедры,
кандидат юридических наук
(Нижегородская академия МВД России)

В статье проводится анализ возможностей интеллектуальных систем при осуществлении уголовно-процессуальной деятельности по расследованию преступлений. Автором обращается внимание на необходимость разработки единого подхода к развитию данного направления интеллектуального обеспечения уголовного процесса и криминалистки.

Интеллектуальное обеспечение, экспертная система, интеллектуальная система, расследование преступлений, база знаний, база данных, принятие решения, доказывание.

Правоприменительная деятельность в своей сущности является крайне сложной и многогранной сферой реализации человеческих способностей и возможностей. В частности, уголовное судопроизводство требует от должностных лиц уголовного процесса не только знаний закона и особого профессионализма, но и значительного интеллектуального потенциала. Однако не всегда правоприменителю следует рассчитывать лишь на свои способности, на свой интеллект. В решении юридических задач, в том числе уголовно-процессуальных, допускается прибегать к использованию не только человеческих ресурсов, но и искусственных интеллектуальных систем, созданных самим же человеком. Их использование в юридической деятельности собственно предопределяется высоким уровнем интеллектуальности, специализации и профессионализма, присущих деятельности юриста, судьи, следователя, криминалиста, судебного эксперта.

Одной из разновидностей таких систем выступает экспертная система, которая представляет интеллектуальную систему, предназначенную для решения задач в определенной предметной области на основе знаний, предоставленных экспертами, которая содержит базу знаний и поддерживает функции обоснования, объяснения и оправдания[1]. В области юриспруденции данные системы также

[1] *Денисова А.А.* Информационные системы и технологии в юридической деятельности: [учеб. пособие]. К.: КНЭУ, 2003. URL: http://lybs.ru/index-841.htm (дата обращения: 07.01.2018).

получили соответствующее применение[1]. Если говорить об интеллектуальной системе поддержки принятия решений в уголовном процессе, то свое развитие она обрела еще в конце прошлого века[2]. Но несмотря на это, устойчивого закрепления не получила до сих пор. Пожалуй, это есть следствие преобладания у правоприменителей консервативных взглядов на форму и содержание процессуальной деятельности – не принятие электронного документооборота, отсутствие доверия к достижениям науки и техники и т. д.

На наш взгляд, такая практика неблагоприятным образом сказывается на уголовно-процессуальной деятельности, на ее качестве, мобильности, стоимости и, главным образом, на назначении. Аргументом такого предположения может выступить то, что любая интеллектуальная система есть результат аккумулирования всех имеющихся знаний в определенной сфере. На это же обстоятельство указывают ряд иных авторов, отмечая, что в экспертных системах человеческий интеллект используется в концентрированном виде для решения стандартных ситуаций в различных областях знаний и что при этом выдаваемые машиной рекомендации носят консультативный характер, принятие решения остается за человеком, хотя эти решения представляют собой качественно новый, более высокий уровень[3].

Как известно, нет такого знания, которое не базировалось бы на уже имеющихся результатах мыследеятельности. Сюда же относится и уголовно-процессуальное и криминалистическое познание преступления. Тем самым отдельной сферой применения экспертных систем является принятие решения о направлении расследования и выполнения следственных действий. При этом сущность криминалистических исследований сводится к установлению закономерности в связях, которые существуют между преступной деятельностью, субъектом преступления, местом и способом совершения преступления, ее следовой картиной. Как отмечает

---

[1] См., например: *Утермен Д.* Руководство по экспертным системам. М., 1989. С. 301–304; *Бессонова А.П.* Экспертные системы в области права // Право и информатика. М.: изд-во Моск. ун-та, 1990. С. 100–107; *Гаврилова Т.А.* Извлечение и структурирование знаний для экспертных систем / Т. А. Гаврилова, К. Р. Червинская. М.: Радио и связь, 1992. 199 с.; *Джарратано Д.* Экспертные системы: принципы разработки и программирование [пер. с англ. и ред. К. А. Птицына]. 4-е изд. М., 2007. 1147 с.; и др.

[2] См., например: *Баранов А. К., Бобрынин Н. Б., Степанов М. Г.* Основы применения вычислительной техники в деятельности органов внутренних дел. Горький: ГВШ МВД СССР, 1987. 93 с.; *Баранов А. К., Цветков С. И.* Компьютерные системы поддержки принятия следователем тактических решений. М.: Академия МВД России, 1992. 112 с.; и др.

[3] Уголовный процесс: учебник для студентов вузов, обучающихся по специальности «Юриспруденция» / под ред. В. П. Божьева. 3-е изд., испр. и доп. М.: Спарк, 2002. С. 29–30.

Г. А. Зорин, подобная экспертная система применительно к деятельности по расследованию уголовных дел включает в себя базу данных, содержащую модели конкретных ситуаций, в которых приходится принимать решения; базу знаний эксперта в виде особых правил – продукций, имеющих форму «если..., то...»; «решателя проблем» («машину логического вывода»), управляющего порядком применения продукции к анализируемой ситуации и выбором рекомендуемого решения[1].

База данных и база знаний, которые в основном содержат теоретические знания и опыт специалистов (на базе их экспертных оценок), образуют «ядро» экспертной системы и при их правильном подборе могут привести к ряду положительных исходов. Например, к ускорению процесса принятия решения конкретной проблемы и нахождения оптимального решения, исходя из имеющихся возможностей (в частности, традиционная экспертная система может позволить молодому следователю либо оперативному сотруднику приступать к работе на уровне специалистов высокого класса); к снижению тактического риска следственного действия, так как перед следователем «проходят» все возможные варианты его деятельности и вероятностные модели взаимодействий; к активизации усвоения ранее полученных знаний и раскрытия новых возможностей решения нестандартных задач; к предоставлению возможности проявлять инициативу и «опережать» партнера, располагая многовариантными моделями решения поставленной задачи (при наличии интеллектуальной мобильности партнера позволяет иметь массу «запасных» откорректированных вариантов, к примеру, программ допроса)[2]. Использование системы также способствует обогащению опыта и знаний сотрудников следственных и оперативных подразделений; установлению так называемых пограничных типов преступников, распознать которых другими методами чрезвычайно трудно или совсем невозможно; устранению некоторой доли субъективизма при формировании версий в условиях неопределенности; выравниванию знаний неодинаково подготовленных сотрудников и т. д.

Знания, содержащиеся в экспертных системах и выраженные в форме правил типа: «Если существует такой факт, то, вероятно, произошло такое действие или существовал такой мотив этого дей-

---

[1] *Зорин Г.А.* Криминалистическая эвристика. Гродно, 1994. Т. II. С. 117.

[2] *Зорин Г.А.* Проблемы применения специальных логико-психологических методов при подготовке и проведении следственных действий: автореф. дис. ... д-ра юрид. наук. М., 1991. С. 24.

ствия», пригодны для автоматизированной обработки и позволяют имитировать процесс оценки следователем ситуации расследования и обеспечивать в режиме диалога консультационную поддержку принятия им решений. Ключевыми задачами, выполняемыми с помощью таких систем, могут выступить: определение возможных направлений расследования (формирование версий о событиях с учетом, по возможности, различных источников получения информации), выбор наиболее вероятных направлений; предоставление пользователю рекомендаций относительно дальнейших действий (назначение экспертиз, проведение оперативно-поисковых мероприятий, проверочные и следственные действия и т. д.).

Необходимо также иметь в виду, что решение этих задач невозможно без наличия таких дополнительных элементов, как: система типовых моделей следственных действий; система тактических приемов, обеспечивающих оптимальность проведения следственного действия; система логических методов, оптимизирующих в традиционных формах решение стандартных следственных задач; система эвристических методов решения следственных задач. Кроме того, следует учесть, что эффективность конкретной экспертной системы зависит от числа и качества типовых программ, введенных в память компьютерной техники, логических и эвристических методов их преобразования, а также числа продукций, содержащихся в ее базе знаний[1].

На сегодняшний день создание экспертных систем в сфере правоприменительной деятельности – явление не новое. «Ближе всего к достижению конкретных устойчивых результатов находятся экспертные системы на основе ЭВМ в области судебной экспертизы, где имеется возможность проводить научные исследования на базе формализации устойчивых, часто встречающихся признаков объектов изучения»[2]. В качестве примеров таких систем можно привести экспертные системы «Наркоэкс» (экспертиза наркотических веществ), «Балэкс» (баллистическая экспертиза), «Кортик» (экспертиза холодного оружия) и т. д. Однако сферой судебных экспертиз применение экспертных систем не заканчивается. Так, существуют экспертные системы, не связанные с производством экспертиз, но направленные на раскрытие и расследование преступлений. Это такие системы, как «Маньяк» – поддержка принятия решений при раскрытии серийных убийств, совершенных на сексуальной

---

[1] *Зорин Г.А.* Криминалистическая эвристика. Гродно, 1994. Т. II. С. 117–118.

[2] Уголовный процесс: учебник для студентов вузов, обучающихся по специальности «Юриспруденция» / под ред. В. П. Божьева. 3-е изд., испр. и доп. М.: Спарк, 2002. С. 29.

почве на основе наиболее вероятной версии о типе возможного преступника с ограничением круга лиц, подлежащих проверке на причастность к определенному преступлению, «Спрут» – устанавливает связи субъектов преступного формирования на основании знаний о преступных формированиях, связей между лицами, экономических составляющих и фактов, представляющих оперативный интерес, и др.

Разумеется, это не весь перечень разработанных наукой и практикой экспертных систем, применимых при расследовании преступлений. Также нельзя утвердительно говорить о совершенстве этих систем. На наш взгляд, на сегодняшний день назрела острая необходимость не элементарного реформирования уголовного процесса, а пересмотра формы и содержания этих реформирований. Полагаем, что в связи с этим разработка рабочих научно-обоснованных экспертных систем принятия уголовно-процессуальных решений и доказывания является хорошим подспорьем, поскольку экспертная система формируется как «концентрат знаний справочного характера», она предоставляет следователю возможность вести с ЭВМ диалог, «советоваться» с ней, искать, перебирать различные варианты, среди которых можно найти наиболее приемлемый или синтезировать несколько вариантов тактических решений, чтобы на их основе построить принципиально новое тактическое решение проблемной следственной ситуации[1]. Но для начала требуется разработать не сами конкретные экспертные системы, а методологию их формирования и применения в практической деятельности.

---

[1] *Зорин Г.А.* Проблемы применения специальных логико-психологических методов при подготовке и проведении следственных действий: автореф. дис. ... д-ра юрид. наук. М., 1991. С. 23.

Особенности тактики проведения различных видов следственного осмотра в ходе расследования развратных действий, совершенных с использованием сети Интернет

К. А. Балашов
(Московская академия Следственного комитета Российской Федерации)

Статья посвящена обнаружению криминалистической значимой информации при расследовании развратных действий в ходе производства различных видов следственных осмотров. Описаны задачи осмотра электронной страницы в социальной сети и мобильных устройств, гаджетов, компьютеров несовершеннолетнего потерпевшего и подозреваемого (обвиняемого), осмотра детализации их телефонных соединений, а также осмотра места жительства несовершеннолетнего потерпевшего.

Интернет, развратные действия, социальная сеть, электронная страница, электронная переписка, компьютерная техника.

Общеизвестно, что под следственным осмотром понимается следственное действие, состоящее в непосредственном восприятии и изучении любых объектов в целях обнаружения, фиксации и изъятии предметов и объектов, имеющих значение для расследования уголовного дела[1]. Данное следственное действие является одним из самых распространенных и проводится практически по всем уголовным делам, имея свои специфические особенности в зависимости от вида преступлений.

В настоящее время уровень развития интернет-услуг позволяет дистанционно вести общение в различных социальных сетях посредством компьютерных устройств, ноутбуков, гаджетов и мобильных телефонов, что способствует появлению новых способов совершения преступлений против несовершеннолетних, в том числе сексуальной направленности. Одним из них является совершение развратных действий путем виртуального общения.

Специфика таких преступлений заключается в том, что они являются одним из видов как половых преступлений, совершенных в отношении несовершеннолетних, так и компьютерных преступле-

[1] *Баев О.Я.* Тактика следственных действий: учебное пособие. М.: Юрлитинформ, 2013. С. 93.

ний, совершаемых с использованием информационно-телекоммуникационных сетей. Данная специфика проявляется в появлении новых объектов следственного осмотра, а также в особенностях его производства.

В ходе расследования указанных преступлений самой распространенной является исходная следственная ситуация, возникающая при поступлении заявления родителя (близкого родственника) об обнаружении сексуальной переписки ребенка (либо о получении им порнографических материалов) в социальной сети (мобильном устройстве)[1]. В связи с чем первоначальный этап расследования развратных действий, совершенных с использованием сети Интернет, необходимо начинать с установления наличия и осмотра зарегистрированной электронной страницы у несовершеннолетнего потерпевшего и подозреваемого, иных страниц, с которых велась интимная переписка, указанная в заявлении и в допросе законного представителя несовершеннолетней потерпевшей. В ходе осмотра электронной страницы можно непосредственно воспринимать содержание общения несовершеннолетнего лица с подозреваемым.

Одной из важнейших задач рассматриваемого следственного действия является поиск и анализ электронной переписки, круга друзей, имеющихся фото и видео, а также сообществ (групп) на странице несовершеннолетнего потерпевшего. Для успешного проведения рассматриваемого следственного осмотра следователю необходимо определить перечень сведений, подлежащих доказыванию по рассматриваемому уголовному делу. Учитывая характер расследуемого преступления и специфику предмета доказывания, можно выделить следующие объекты, подлежащие осмотру, и обстоятельства, которые можно установить.

История электронной переписки несовершеннолетней в социальных сетях позволит выявить круг общения, установить свидетелей и выявить новых несовершеннолетних потерпевших. Например, в ходе осмотра истории общения несовершеннолетнего потерпевшего Д. была обнаружена переписка с другими пользователями, с которыми он делился общением на интимные темы с подозреваемым Р.[2]

2. Фотографии, содержащиеся на странице несовершеннолетнего потерпевшего, по которым можно установить, кто изображен

---

[1] *Антонов О.Ю.* Типичные следственные ситуации при расследовании сексуальных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей: специфические особенности и пути разрешения // Российский следователь. 2018. № 2. С. 4.

[2] См.: Обвинительное заключение по уголовному делу № 0240027 следственного отдела по Московскому району СУ СК России по Тверской области.

на фотографии, количество сохраненных и оправленных обнаженных фотографий, на которых изображен несовершеннолетний потерпевший, в одежде или без изображен несовершеннолетний потерпевший, дата и время сохранения фотографий на странице. Кроме того, следователю необходимо обращать внимание на обстановку, в которой были изготовлены фотографии с изображением несовершеннолетнего потерпевшего. В целях дальнейшей возможной идентификации места съемки необходимо обращать внимание на задний фон фотоснимка, который может содержать элементы обстановки.

Вторым видом следственного осмотра является осмотр мобильных устройств, гаджетов, компьютеров несовершеннолетнего потерпевшего в целях поиска и изучения текстового электронного общения интимного содержания с подозреваемым либо обменом и отправкой несовершеннолетним потерпевшим своих «обнаженных» фотографий[1].

Осмотр компьютерной техники проводится в целях поиска и изучения текстового электронного общения интимного содержания с подозреваемым либо обменом и отправки несовершеннолетним потерпевшим своих «обнаженных» фотографий.

Например, в ходе осмотра предметов был осмотрен ноутбук, принадлежащий потерпевшему Р., который использовал для выхода в сеть интернет, для общения с подозреваемым Т., на котором были обнаружены обнаженные фотографии подозреваемого Т., а также интимная переписка, содержащая дату и время получения и отправления[2].

По мнению некоторых авторов, ранее описанный осмотр страницы в социальной сети, которой пользовался потерпевший и с помощью которой совершено преступление, является элементом осмотра компьютера потерпевшего[3].

Третий вид следственного осмотра – осмотр места происшествия, в качестве которого выступает место жительства несовер-

---

[1] *Бахтеев Д.В.* Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети Интернет // Российский следователь. 2017. № 21. С. 12.

[2] См.: Обвинительное заключение по уголовному делу № 024006 следственного отдела по Московскому району СУ СК России по Тверской области.

[3] *Каримов Р. М., Кайгородов А. С.* Особенности производства первоначальных следственных действий по делам о преступлениях против половой неприкосновенности несовершеннолетних, совершенных с использованием сети Интернет (ст. 132, 135 УК РФ) // Современные проблемы предупреждения, выявления, пресечения и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий: материалы научно-практического семинара-совещания (Екатеринбург, март 2017 г.) / отв. ред. В. Н. Карагодин. Екатеринбург, 2017. С. 78.

шеннолетнего потерпевшего, необходимо проводить как в комнате, в которой проживает несовершеннолетний потерпевший, так и в других местах жилого помещения, которые имеют доступ в сеть Интернет. Задача проведения осмотра места происшествие заключается в идентификации обстановки, в которой были изготовлены обнаженные фотографии (видеозаписи) несовершеннолетнего потерпевшего. С помощью изображенной на них обстановки в ходе осмотра места жительства потерпевшего можно установить место, в котором была проведена данная съемка. Что позволит провести дополнительный осмотр для обнаружения и выявления новых следов преступления.

Наряду со следственным осмотром, проведенным с участием несовершеннолетнего потерпевшего, по аналогичной схеме следует произвести еще два вида следственного осмотра – осмотр мобильных устройств и компьютерной техники, используемой подозреваемым, а также его электронных страниц в социальных сетях.

Первый может установить:

– историю переписки;

– посещения порносайтов или загрузок фото, видеофайлов порнографического содержания;

– поиск и посещение страниц несовершеннолетних потерпевших;

– лицо в совершении преступления (видео, фото совершенного преступления, смс-сообщения о совершенном преступлении);

– возможность причастности его к совершенному преступлению (закладки на соответствующих сайтах, пометки в календаре, переписка, опровержение алиби и т. д.).

Второе может установить:

– интернет-сайтов;

– содержание переписки в различных социальных сетях;

– последние поисковые запросы;

– контакты в социальных сетях, с кем подозреваемый осуществлял общения;

– графические файлы с изображением обнаженного несовершеннолетнего потерпевшего и подозреваемого.

Осмотр электронной страницы, зарегистрированной под вымышленным и (или) реальным именем подозреваемого, позволяет установить следующие сведения:

– факт преступной переписки между несовершеннолетней потерпевшей и подозреваемым;

– обмен фотографиями и видеозаписями, содержащими интимный характер;

– место съемки и видеозаписи, на котором изображен сам подозреваемый;

– место и время выхода подозреваемого в сеть Интернет;

– технические и мобильные устройства, используемые как подозреваемым, так и несовершеннолетним потерпевшим;

– факты распространения порнографических материалов конкретного потерпевшего другим лицам;

– новые преступные эпизоды, совершенные в отношении других несовершеннолетних потерпевших.

Последним видом следственного осмотра является осмотр детализации телефонных соединении между подозреваемым и несовершеннолетним потерпевшим. С помощью рассматриваемого следственного действия можно доказать причастность лица к совершению развратных действий с использованием сети Интернет, даже без осмотра мобильного устройства подозреваемого.

Например, в ходе осмотра полученной детализации абонентских соединений подозреваемого Ю. было установлено время и дата входящих и исходящих телефонных соединений с несовершеннолетней потерпевшей Н., а также отправленных и полученных смс-сообщений интимного характера[1].

Таким образом, значение рассмотренных видов следственных осмотров в рамках расследования развратных действий, совершенных с использованием сети Интернет, заключается в доказывании объективной стороны преступления, выражающейся в переписке на сексуальную тему и обмене «обнаженными» фотографиями между подозреваемым и несовершеннолетним потерпевшим в определенное время с использованием определенных средств компьютерной техники, установлении лица, совершившего развратные действия, возможных свидетелей преступления, а также может способствовать выявлению нового несовершеннолетнего потерпевшего или дополнительного эпизода преступной деятельности[2].

---

[1] См.: Обвинительное заключение по уголовному делу № 15080085 следственного отдела по Заводскому району СУ СК России по Кемеровской области.

[2] См. подробнее: *Антонов О.Ю.* Выявление дополнительных эпизодов и новых видов порно-сексуальной преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. 2017. № 3. С.173–177.

Криминалистическая классификация цифровой доказательственной информации

Д. В. Бахтеев,
доцент кафедры криминалистики,
кандидат юридических наук
(Уральский государственный
юридический университет)

В статье рассматриваются признаки цифровой (электронной) информации, различные подходы к классификации цифровой информации, которая может иметь доказательственное значение с точки зрения формы носителя, способа доступа, сложности доступа, характера происхождения, места нахождения, формы представления, типа устройства, формы, целевого предназначения. Рассматриваются формы информации, размещенной в сети Интернет. Анализируется классификационная система вредоносного программного обеспечения.

Цифровая информация, электронная информация, вредоносное программное обеспечение.

XXI век для человеческой цивилизации вполне можно назвать цифровой эпохой. Трудно переоценить значение цифровых технологий для практически всех сфер человеческой деятельности. Экспоненциально возрастает разнообразие форм, средств и методов обработки цифровой информации, увеличивается ее общий объем, что зачастую способствует не только общественно одобряемым операциям с информацией, но и может иметь непосредственное отношение к преступной деятельности. Криминалистика, всегда находившаяся на острие борьбы с преступностью, должна адаптироваться к изменяющимся условиям, что требует не просто совершенствования, но и постоянного обновления криминалистических знаний о технико-тактических аспектах операций с цифровой доказательственной информацией в процессе выявления, раскрытия и расследования преступлений.

Предметом криминалистики всегда выступали операции со следовой информацией. Следы, как носители такой информации, при этом дифференцировались исходя из их носителя: на материальные и идеальные.

К материальным следам относятся любые объекты материальной действительности, способные на физическом или химическом

уровне взаимодействовать друг с другом (пули, гильзы, следы рук, обуви, крови и т. д.). Восприятие такой информации, как правило, осуществляется непосредственно, она носит достаточно точный и проверяемый характер.

Идеальные следы, в свою очередь, включали в себя мысли, воспоминания, ощущения, то есть отражение объективной действительности в сознании человека, проявляющиеся, как правило, при вербальных действиях в речи человека (при допросе, проверке показаний на месте и т. д.). Информация, закодированная в таких следах, воспринимается всегда опосредованно и подвержена ошибкам и искажениям.

Место в этой системе цифровой информации, появившейся в XX в. и получившей бурное развитие в XXI в., до сих пор окончательно не определено. С одной стороны, она обладает свойствами материальных следов, поскольку с физической точки зрения представляет собой характеристику носителя информации, например уровень намагниченности участка поверхности жесткого диска или электрический заряд в транзисторах твердотельных накопителях (флеш-карты, SSD-диски). С другой стороны, цифровая информация не может восприниматься субъектом познания (например, следователем) непосредственно: для ее обнаружения и исследования требуются технические устройства, равно как для осуществления операций с идеальной информацией необходимой является ее передача от человека, который ею владеет. Таким образом, цифровая информация с криминалистической точки зрения обладает двойственной природой и в целях настоящей работы может быть представлена в качестве третьего вида следовой информации, используемой при раскрытии и расследовании преступлений.

С точки зрения В. Б. Вехова, цифровая (или компьютерная) информация обладает набором следующих характеристик:

– цифровая информация является одной из объективных форм существования информации – электронной формой;

– она всегда опосредована через материальный носитель, вне которого физически не может существовать;

– доступ к компьютерной информации могут иметь одновременно несколько лиц;

– такая информация достаточно просто и быстро преобразуется из неэлектронных форм в электронные и обратно;

– копируется на любые носители и пересылается на практически любые расстояния;

– собирается, исследуется и используется только с помощью специальных технических средств[1].

Добавим также, что в подавляющем большинстве случаев цифровая следовая информация обезличена, что ставит перед органами следствия и дознания дополнительную задачу по соотнесению отдельного цифрового следа с лицом, имеющим отношение к событию преступления. Соответственно, под цифровыми следами следует понимать разновидность цифровой (компьютерной) информации, связанной с событием преступления. Рассматриваемую категорию следов нельзя полноценно отнести ни к материальным, ни к идеальным следам: такие следы невозможно изучать непосредственно, однако их исследование осуществляется с помощью технических, а не логико-психологических средств и методов.

Цифровые следы как носители криминалистически значимой доказательственной информации могут быть классифицированы по различным основаниям. Рассмотрим такие классификационные системы.

Первым основанием классификации цифровых следов может по праву выступить форма их носителя. Согласно этому основанию цифровые следы могут быть расположены на оптических носителях (CD, DVD, Blue-Ray диски и пр.), полупроводниковых носителях (флеш-память, SSD-носители и магнитных носителях (жестких дисках).

Другим основанием деления цифровых следов является способ осуществления доступа к ним. Доступ к цифровой информации может осуществляться локально либо удаленно. В первом случае доступ осуществляется непосредственно через устройство, содержащее носитель, на котором находятся цифровые следы. При этом возможен весь комплекс криминалистических операций по обнаружению, фиксации, изъятию и исследованию следов. При расположении искомой информации на удаленном носителе доступ к ней осуществляется при дополнительном использовании подключения к телекоммуникационным сетям. При этом исключается изъятие следов в традиционном криминалистическом понимании, однако они могут быть скопированы на иной носитель.

---

[1] *Вехов В.Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: сб. науч.-практ. тр. М.: Академия Следственного комитета Российской Федерации, 2016. № 1. С. 156.

По характеру сложности доступа цифровые следы могут быть доступными (например, электронные документы), скрытыми (скрытые файлы, информация, скрытая с помощью методов стеганографии) и зашифрованными. В последнем случае сам факт наличия информации очевиден субъекту расследования, однако доступ к ее содержанию затруднен, как правило, с помощью паролей или иных средств идентификации или аутентификации ее создателя или владельца.

По характеру происхождения цифровые следы дифференцируются на оставленные человеком непосредственно (электронные документы, записи в социальных сетях и т. п.) и опосредованно (данные телеметрии, системные логи, атрибуты создаваемых файлов (время, пользователь, размер и пр.) и т. п.). Следы первой группы могут быть изучены следователем в ходе следственных действий (как правило, следственного осмотра), вторая же группа требует использования специальных знаний (как правило, производства компьютерно-технических исследований).

По месту нахождения цифровые следы могут находиться на компьютерных устройствах во владении преступника (например, исходный код вредоносного программного обеспечения или шаблоны для изготовления подложных документов), на устройствах потерпевшего (например, функционирующее вредоносное программное обеспечение), устройствах сторонних лиц (например, электронная почта на сервере организации, предоставляющей услуги такого рода). Разумеется, цифровые следы могут зачастую одновременно располагаться на носителях, относящихся ко всем трем группам. В данном группе отдельно стоит выделить информацию, размещенную в сети Интернет. С точки зрения формы размещения, информация в сети Интернет может быть классифицирована следующим образом:

– публикации на веб-сайтах;

– файлы, хранящиеся в пиринговых (файлообменных) сетях;

– информация, передаваемая напрямую в потоковом режиме в реальном времени посредством телеконференций (трансляций, вебинаров, чатов и т. д.)[1].

С точки зрения формы представления, большинство цифровых следов относятся к текстовой информации, однако в следственно-судебной практике встречаются случаи использования следов в форме графической или звуковой цифровой информации.

---

[1] Электронные носители информации в криминалистике: монография / под ред. О. С. Кучина. М.: Юрлитинформ, 2017. С. 176.

Согласно типу устройства, на котором находятся цифровые следы, можно выделить стационарные (сервера, персональные стационарные компьютеры, стационарные веб-камеры) и мобильные устройства, к которым относятся смартфоны, планшеты, ноутбуки, фотокамеры, навигаторы и пр. Следует учитывать, что доказывание связи цифровых следов с конкретным лицом всегда зависит от типа устройства и в некоторых случаях может быть усложнено. Так, например, подозреваемый может заявить, что доступ к его персональному компьютеру имела группа людей; стороной защиты может быть выдвинута версия о том, что учетная запись обвиняемого в социальной сети была взломана третьими лицами и т. д.

По своей форме цифровые следы могут представлять отдельную программу, комплекс программ, банки и базы данных, электронные сообщения, отдельные файлы, веб-сайты или отдельные их страницы и т. д.

С точки зрения целевого предназначения программы могут быть ориентированы на выполнение полезных или вредных функций. Для современной криминалистики большой интерес представляет обособленный класс программ – зловредное программное обеспечение (Malware). «Механизм его работы сводится либо к прямому воздействию на программную среду, если оно технически осуществимо (отсутствуют средства ограничения доступа), либо к использованию дефектов аппаратного и программного обеспечения, либо к атакам типа «отказ в обслуживании», которые заключаются в перегрузке оборудования, так что оно не может выполнять свои функции»[1]. К основным видам таких программ относят:

– трояны, предоставляющие преступнику доступ к управлению компьютером, операциям, производимым на компьютере или пользовательской информации. К троянам могут относиться перехватчики камеры и клавиатуры, устройства для обнаружения паролей и чтения электронных сообщений. До недавнего времени именно трояны считались наиболее опасной формой зловредного программного обеспечения;

– вирусы, задачей которых является повреждение функций компьютера (к примеру, уничтожение системных или пользовательских файлов, загрузочных секторов системных дисков и пр.);

---

[1] *Гребеньков А.А.* Современное состояние проблемы вредоносного программного обеспечения: основы компьютерной криминальной армалогии // Известия Юго-Западного государственного университета. 2014. № 6 (57). С. 162.

– программы-вымогатели (ransomware) представляют собой разновидность вирусов, задачей которых является уже не простое повреждение компьютера потерпевшего, а вымогательство выкупа под угрозой уничтожения или безвозвратного повреждения (обычно в форме шифрования). В мае 2017 г. программа Wana Decrypt0r 2.0 нанесла мировой экономике ущерб, оцениваемый в 1 млрд долларов США, от ее атаки пострадали более 500 тыс. пользователей и 200 тыс. IP-адресов.

Изучение различных форм существования цифровой доказательственной информации позволит правоохранительным органам адаптироваться к изменяющимся условиям жизни в эпоху значительных технологических изменений.

Аэромобильные комплексы как новое средство повышения эффективности обнаружения и фиксации информации

А. В. Бецков,
доктор технических наук, доцент
(Академия управления МВД России)

В статье рассматриваются вопросы использования аэромобильных комплексов для получения достоверной информации о правонарушениях.

Аэромобильный комплекс, высотная аэромобильная платформа, оперативное управление, летательный аппарат, беспилотные летательные аппараты, бортовой комплекс технических средств, средства сбора криминалистической информации.

Министр внутренних дел Российской Федерации, несмотря на значительные положительные результаты в борьбе с преступностью, достигнутые в последние годы, и общее состояние дел в этой сфере, требует повышения эффективности деятельности органов внутренних дел, и эта проблема сегодня является государственной. Это обусловлено прежде всего недостаточно эффективной системой сдерживания, предупреждения, профилактики и пресечения преступлений, их качественного расследования, должного информационного обеспечения сил правопорядка о замышляемых и совершаемых правонарушениях.

Расширение сфер влияния, масштабности деятельности экстремистских и террористических организаций, преступных сообществ, увеличение числа преступлений и правонарушений, таких как массовые беспорядки, групповые нарушения общественного порядка, внутренние вооруженные конфликты, действия незаконных вооруженных формирований, характеризующихся особой опасностью, решительностью, дерзостью, организованностью и вызывающих большой общественный резонанс, требует от правоохранительных органов повышения эффективности управления силами и средствами в любой обстановке, улучшения работы действующей системы органов управления, существенного повышения оперативности и появившиеся новые разрешающие возможности[1].

[1] О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ // Рос. газ. 2011. 8 февр.

Научное исследование на тему «Теоретические, организационные и правовые основы формирования и функционирования аэромобильных комплексов МВД России», начатое в 2007 г. как диссертация на соискание ученой степени доктора наук, продолжается и в настоящее время[1]. На достоверность материалов, получаемых в ходе исследования, оказывали объективные факторы, поддерживающие высокий научно-практический интерес к данному изысканию. По мнению автора, к факторам, способствующим высокому уровню актуальности и достоверности научной работы, можно отнести: достаточно длительный временной период разработки темы, неоднозначная и сложная оперативная обстановка, реформа правоохранительной системы в целом и МВД России в частности, научно-технический прогресс, позволяющий обосновывать принципиально новые решения, а также аргументированные требования высшего руководства страны и Министра внутренних дел Российской Федерации, направленные на совершенствование обслуживания населения за счет применения инновационных технологий.

В процессе исследовательской работы проводилось социологическое исследование в виде анкетирования, интервьюирования и экспертного опроса руководителей территориальных органов МВД России различных уровней. В социологическом исследовании приняло участие более двух тысяч сотрудников указанной категории, ученых, практических специалистов данного направления деятельности. Отмечено, что ответы на такие вопросы как: «Считаете ли возможным применять летательные (воздухоплавательные) аппараты, оборудованные специальными техническими средствами связи, видео, фото, радио, лазерного, акустического контроля для разведки, мониторинга обстановки и доведения сигналов управления до сил и средств МВД России?», «Считаете ли Вы, что размещение органа оперативного управления на АМК существенно расширит его возможности по управлению силами и средствами МВД России?», «Считаете ли Вы возможным использовать АМК как орган оперативного управления силами и средствами ОВД при резком обострении оперативной обстановки?» – давали положительный ответ на поставленный вопрос порядка 80–90 % респондентов на начальной стадии социологического исследования. Представителям высшего руководящего состава МВД России было предложено

[1] *Бецков А.В.* Теоретические и организационные основы формирования и функционирования аэромобильных комплексов МВД России. М.: Академия управления МВД России, 2009. С. 198.

Бецков А.В. Формирование и функционирование аэромобильных комплексов МВД России. М: Академия управления МВД России, 2010. С. 237.

ответить еще на ряд вопросов, связанных с возможностью формирования и функционирования АМК. Анализ результата ответов показал, что со временем все больше респондентов поддерживает не только применение АМК в системе МВД России[1], но и согласны, что они позволят сформировать высокомобильные силы постоянной готовности, и позволят значительно расширить возможности ОВД по противодействию преступлениям на ранних стадиях их совершения.

Сформированы основы научной теории о создании и применении АМК в интересах ООП и ООБ. Был разработан учебно-методический комплекс для обучения в Академии управления МВД России руководящего состава территориальных органов МВД России вопросам организации применения и непосредственного использования АМК при противодействии преступлений. Авторский коллектив углубленно исследовал результаты использования АМК.

Детальному анализу подверглись материалы непосредственной практической деятельности АОСН и их отчетные результаты в статистической форме.

Исходя из анализа основных статистических данных ГИАЦ МВД России о результатах оперативно-служебной деятельности с применением АМК за период 2010–2015 гг., целесообразно отметить следующие выявленные закономерности: эффект носит нелинейный характер, т. е. полезность может не постоянно сопровождать регулярные расходы на содержание системы, однако применение одноразового применения может оправдать экономическую целесообразность; наличествует экономический эффект от АМК; совокупный объем выполненных авиационных работ (количество вылетов, время налета, объем перевозок) прямо пропорционально влияет на результаты выявления и раскрытия преступлений. Увеличение объема авиационных работ в интересах оперативно-служебной деятельности способствует повышению эффективности выявления и раскрытия преступлений; увеличение интенсивности и объема полезных авиационных работ в интересах оперативно-служебной деятельности, в т. ч. использование как средство оперативного получения уникальной криминологической информации.

Таким образом, проанализировав основные результаты оперативно-служебной деятельности АМК в структуре АОСН за время

---

[1] *Бецков А.В.* Теоретические и организационные основы формирования и функционирования аэромобильных комплексов МВД России. М.: Академия управления МВД России, 2009. С 198.

Бецков А.В. Формирование и функционирование аэромобильных комплексов МВД России. М: Академия управления МВД России, 2010. С. 237.

существования в XXI в., мы пришли к выводу, что этот вид специальных подразделений обладает уникальными возможностями, использование которых приносит существенную пользу правоохранительной деятельности МВД России.

На современном этапе правоохранительной деятельности подразделения по охране общественного порядка нуждаются в уникальных тактико-технических характеристиках, которыми обладают АМК. Возможности АМК крайне необходимы системе МВД России. Существенное значение имеет организация качественного применения в интересах криминалистической деятельности ОВД, противодействию преступности на территории Российской Федерации[1].

По мнению автора, сегодня актуальна проблема оснащения подразделений МВД России, задействованных в противодействии преступности и охране общественного порядка, аэромобильными комплексами. Структура АМК МВД России может иметь типовой вид, зависящий от целевой задачи, включающий в себя структурные компоненты и элементы[2].

Формирование и функционирование АМК может осуществляться в организационной структуре территориального органа федерального органа исполнительной власти соответствующего уровня. Все задачи, возложенные на АМК, можно разделить на два основных блока. К первому относятся задачи заблаговременного обеспечение готовности компонентов и элементов АМК. Ко второму блоку относятся задачи по непосредственному функционированию АМК в режиме сбора, фиксации, обработки, хранения информации и доведения сигналов управления до территориальных органов внутренних дел МВД России при осложнении оперативной обстановки.

Научная новизна данного подхода заключается не только в возможном реагировании на потребность объективную – провести такого рода исследования, направленного на повышение оперативности и качественности информированности уполномоченных органов и подразделений о ранних стадиях событий криминального и правового характера.

---

[1] *Долинко В.И.* Анализ рисков и угроз в системе материально-технического снабжения органов внутренних дел Российской Федерации в особых условиях и методы их снижения: Труды Академии управления МВД России. 2012. № 2 (22). С. 111–114.

[2] *Бецков А.В.* Теоретические и организационные основы формирования и функционирования аэромобильных комплексов МВД России. М.: Академия управления МВД России, 2009. С. 198.

Возможность комплексного использования указанных разрешающих возможностей создает иную качественную характеристику системе управления и в совокупности имеет еще одну разрешающую возможность для оперативного штаба: возможность превращать АМК (при необходимости) в самостоятельный пункт управления, способный оперативно перемещаться в пространстве, непрерывно проводя мониторинг обстановки, маневрировать, управлять силами и средствами МВД России с учетом поставленных задач, обнаруживать преступников, задерживать и доставлять на место постоянной дислокации ОВД, обеспечивать собственную и системную безопасность компонентов[1], применяя, при необходимости, вооружение, специальные средства и информационные технологии[2].

[1] *Долинко В.И.* Комплекс мер по обеспечению экономической безопасности тыла органов внутренних дел: Труды Академии управления МВД России. 2016. № 4 (40). С. 63–67.

[2] *Бецков А.В.* Формирование и функционирование аэромобильных комплексов МВД России. М: Академия управления МВД России, 2010. С. 237.

Предварительная проверка по материалам, связанным с незаконным оборотом оружия и боеприпасов, распространяемых в информационно-телекоммуникационных сетях

Е. В. Блинова,
преподаватель кафедры
предварительного расследования
(Московский университет МВД РФ
им. В. Я. Кикотя)

Данная статья посвящена содержанию доследственной проверки по материалам, связанным с незаконным оборотом оружия и боеприпасов, распространяемых в информационно-телекоммуникационных сетях, то есть алгоритму действий при ее проведении, а также документальному результату, с которым предстоит работать следователю, дознавателю, на основании которых будет приниматься решение в порядке ст. 144 УПК РФ.

Проверка по заявлению, информационные сети, незаконный оборот оружия, расследование.

За январь – декабрь 2017 г. в Российской Федерации было зарегистрировано 1 551 600 преступлений. Количество выявленных преступлений, связанных с незаконным оборотом оружия, по сравнению с аналогичным периодом 2016 г., увеличилось на 2,3 % и составило 22 700, а количество выявленных фактов хищения и вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств уменьшилось на 8,3 % (929 преступлений). В 2017 г. с использованием оружия совершено 4 000 преступлений (-7,9 %). Наибольшее количество зарегистрированных преступлений данной категории отмечается в Свердловской области (186), Краснодарском крае (159), г. Москве (147), Республике Дагестан (145), Московской области (129)[1].

Для того чтобы начать предварительную проверку по материалам, связанным с незаконным оборотом оружия и боеприпасов, распространяемых в информационно-телекоммуникационных сетях, необходима отправная точка. В. Н. Григорьев отмечает, что «деятельность по непосредственному обнаружению признаков престу-

[1] Интернет-ресурс: https://мвд.рф/folder/101762/item/11341800 (дата обращения: 18.04.2018).

пления, предварительная проверка начинается с получения какой-либо информации»[1].

Подобная информация побуждает должностных лиц правоохранительных органов провести проверку, чтобы установить действенное событие и оценить его с точки зрения противоправности. Анализ содержания ч. 1 ст. 144 УПК РФ (в редакции от 4 марта 2013 г.) позволяет выделить следующие виды организационно-правовых форм ее проведения: предварительная проверка сообщений о преступлении и производство первоначальных следственных и иных процессуальных действий при расследовании преступлений, в зависимости от их правовой природы. Таковыми в основном являются непроцессуальные формы (оперативная проверка – проведение оперативно-розыскных мероприятий) и уголовно-процессуальные формы (предварительная проверка сообщений о преступлении и предварительное расследование)[2].

Более сложный для выявления и раскрытия – это бесконтактный способ сбыта оружия и боеприпасов к нему, который стал возможен благодаря повсеместному распространению и доступности интернета.

Схематично представим этот способ совершения преступлений рассматриваемой категории так. Злоумышленник, а чаще группа злоумышленников, создает сайт в сети Интернет с предложением соответствующего характера. При этом может как прямо предлагаться товар, так и делаться это завуалировано. Им же может быть размещено объявление на уже существующем и функционирующем сайте.

Таким образом, заинтересованное лицо – потенциальный покупатель – может заказать покупку посредством стационарного компьютера или через мобильный телефон. Далее покупатель оплачивает покупку путем перевода денежных средства на указанный в объявлении или на сайте счет электронной системы оплаты. В качестве систем оплаты используются повсеместные «киви-кошельки», откуда злоумышленниками денежные средства переводятся на другие номера электронных платёжных систем либо на банковские счета физических лиц. Также денежные средства могут быть переведены на счета юридических лиц, после чего происходит их обналичивание.

---

[1] *Григорьев В.Н.* Возбуждение уголовного дела при непосредственном обнаружении признаков преступления // Правоведение. М., 1982. С. 98.

[2] *Рагулин И.Ю.* Организационные аспекты методики расследования незаконного оборота оружия и боеприпасов: автореф. дис. ... канд. юрид. наук. Краснодар, 2016. С. 19.

Эффективность деятельности оперативных сотрудников по выявлению и документированию незаконного оборота оружия, совершенного с использованием сети Интернет, в значительной степени определяется уровнем ее информационной и аналитической составляющей. При этом незаконный сбыт оружия, совершенный посредством сети Интернет, характеризуется высоким уровнем латентности, обусловленной отсутствием в указанной категории уголовных дел «потерпевшего».

В связи с вышесказанным значительной представляется роль оперативно-разыскной работы при выявлении и раскрытии незаконного оборота оружия, совершаемого бесконтактным способом, а именно путем получения оперативно значимой информации о лицах, занимающихся такого рода преступлениями. Осуществив проверку такой информации и проведя комплекс ОРМ, сотрудники полиции смогут выявить конкретное преступление.

Первичная информация о незаконном обороте оружия, совершенном с использованием сети Интернет, поступает оперативным сотрудникам от лиц, оказывающих конфиденциальное содействие органам внутренних дел, ранее судимых за аналогичные преступления, а также от сотрудников других служб и подразделений правоохранительных органов, которые получили ее в результате осуществления своей служебной деятельности или посредством получения объяснений от задержанных, с указанием источника приобретения оружия. Немаловажным источником информации может быть мониторинг тематических или близких по тематике сайтов и форумов, рекламных и торговых сетевых площадок[1].

Получение и анализ информации об интернет-магазинах, осуществляющих завуалированно незаконный оборот оружия и боеприпасов, а также лицах, дающих такие объявления, позволяет оперативным путем установить информацию об электронном счете, на который требуется перевести деньги. Такой счет привязан к платежному сервису «киви-кошелек».

По результатам проверки первичной информации оперативные сотрудники проводят комплекс ОРМ, направленных на документирование рассматриваемой категории преступлений.

Итак, доследственная проверка по незаконному обороту оружия и боеприпасов к нему будет включать следующие действия.

---

[1] *Бычков В.В.* Криминальный оборот оружия и боеприпасов: понятие, квалификация и расследование: учебное пособие. М.: Юрлитинформ, 2015. С. 133.

Прежде всего необходимо направить соответствующий запрос в «Киви Банк», чтобы установить возможные варианты движения денежных средств с такого счета. Параллельно проводится работа по определению и отслеживанию средств связи, используемых предполагаемыми преступниками, что позволит установить личности всех членов группы, занимающейся незаконным оборотом оружия в сети Интернет. В процессе документирования возможно задержание лица, приобретающего «закладку», в месте ее нахождения.

Задержание покупателя в данном случае может не помочь установить сведения о сбытчике. В таком случае при опросе задержанного необходимо: выяснить способ приобретения оружия или боеприпасов к нему, интернет-ресурс, логин продавца на интернет-ресурсе; наличие в памяти мобильного телефона задержанного переписки с продавцом; способ оплаты; был ли оставлен комментарий при перечислении денег на «киви-кошелек».

После возбуждения уголовного дела в результате проверки возможно проведение в рамках данного уголовного дела ряда следственных действий.

В юридической литературе существует мнение, что «реализация оперативной информации» целесообразна лишь после выявления всего механизма незаконного оборота оружия и лиц, вовлеченных в незаконную деятельность.

Таким образом, предварительная проверка материалов о незаконном обороте оружия и боеприпасов к нему, совершаемых с использованием сети Интернет, осуществляется посредством проведения ОРМ. Помимо приведенных мероприятий проводится также оперативно-разыскное мероприятие «обследование помещений, зданий, сооружений, участков местности и транспортных средств»[1].

Для документирования незаконного оборота оружия, совершенного бесконтактным способом, дополнительно проводится ОРМ «наблюдение», объектом которого является поведение лица, производящего закладку. Проведение этого ОРМ обычно фиксируется при помощи средств аудио – и видеозаписи.

Такое оперативно-разыскное мероприятие, как «прослушивание телефонных переговоров», проводится в ходе документирования бесконтактно совершаемого незаконного оборота оружия

[1] *Скоропупов Ю. И.* К вопросу об уголовно-правовых и криминалистических аспектах характеристики незаконного оборота оружия, его основных частей и боеприпасов // Вестник Тульского государственного университета. 2016. С. 45.

и боеприпасов к нему в случае, если известны члены преступной группы и используемые ими абонентские номера. Кроме того, это ОРМ осуществляется, если общение покупателя с продавцом ведется посредством смс-сообщений. Так, если не удается обнаружить заложенное оружие, возможен телефонный контакт с продавцом для уточнения места закладки.

В ходе доследственной проверки при выявлении незаконного оборота оружия, совершенного бесконтактным способом, практически всегда проводится такое оперативно-разыскное мероприятие, как «снятие информации с технических каналов связи». Таким образом фиксируется интернет-переписка сбытчиков и установления IP-адресов используемых ими технических средств.

Способы неправомерного завладения компьютерной информацией, передаваемой посредством электронной почты

С. Н. Веснина,
начальник кафедры,
кандидат юридических наук, доцент
(Владивостокский филиал
Дальневосточного юридического института
МВД России)

А. В. Неустроева,
доцент кафедры,
кандидат юридических наук
(Владивостокский филиал
Дальневосточного юридического института
МВД России)

Е. В. Жидкова,
старший преподаватель кафедры
(Владивостокский филиал
Дальневосточного юридического института
МВД России)

В статье рассматриваются особенности подготовки к совершению преступлений, предметом преступного посягательства которых является компьютерная информация, передаваемая посредством электронной почты, что позволяет определить локализацию следов преступления.

Компьютерная информация, электронный документ, способ совершения преступления, подготовка.

Современная действительность характеризуется широким использованием информационно-телекоммуникационных технологий практически во всех сферах общественных отношений. В наши дни сложно представить экономическую, да и многую другую деятельность без современных платежных систем, без компьютерной техники, без информационно-телекоммуникационных сетей, информационных систем, электронного документооборота, а также социальных сетей и иных средств общения вне зависимости от временных и территориальных границ. Возможности цифровой техники и циф-

ровых технологий в полной мере позволяют повысить экономическую активность различных хозяйствующих субъектов, положительно влияя в конечном итоге на рост их капиталов. Соответственно, эти процессы не могут остаться без внимания криминалитета, использующего информационное пространство, информационные и телекоммуникационные технологии в своих корыстных целях.

Изложенное диктует необходимость обращения пристального внимания на криминалистическое обеспечение раскрытия и расследования преступных посягательств в данной сфере.

По преступлениям данной категории в качестве основного источника доказательств используется компьютерная информация, в том числе электронные документы.

Понятие информации дано в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», согласно которой ею являются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления[1].

Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[2]. Анализ буквального толкования указанных норм приводит к выводу о несовершенстве используемых формулировок. Так, апеллируя к термину «компьютер», М. В. Старичков справедливо определяет «компьютерную информацию как зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах»[3].

Электронный документ – это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах[4].

---

[1] Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 19.02.2018) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[3] *Старичков М.В.* Понятие «компьютерная информация» в Российском уголовном праве. URL: https://cyberleninka.ru/article/v/ponyatie-kompyuternaya-informatsiya-v-rossiyskom-ugolovnom-prave.

[4] Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс».

Использование сотрудниками правоохранительных органов информации, в том числе компьютерной, в процессе раскрытия и расследования преступлений, предполагает как минимум понимание особенностей, связанных с ее собиранием, хранением, обрабатыванием, предоставлением для пользователей, а также процессом ее распространения. Следует учитывать, что информация может быть уничтожена как по причине случайного стечения обстоятельств, так и при целенаправленных действиях преступников.

Лица, совершающие преступления, связанные с компьютерной информацией, как правило, обладают серьезными знаниями в этой сфере, высокой квалификацией и даже изобретательностью. Соответственно, чтобы успешно противодействовать этому виду преступных проявлений, сотрудники правоохранительных органов, прежде всего следователи, оперативные работники, должны владеть методикой расследования преступлений в сфере информационных технологий, в число основных элементов которых входит криминалистическая характеристика.

Развернувшаяся с середины 60-х гг. прошлого века в криминалистической литературе полемика, связанная с введением А. Н. Колесниченко в криминалистику термина «криминалистическая характеристика преступления»[1], относительно понятия ее сущности и места в науке, давно затихла и данное понятие прочно заняло основное место в системе частных криминалистических методик. Споры, касающиеся элементов, составляющих ее содержание, также постепенно утихли, при этом не достигнув единства взглядов на ее структуру. Не останавливаясь на вопросах теоретического характера относительно понятия и структуры криминалистической характеристики преступления, учитывая, что способ совершения преступления как элемент, входящий в криминалистическую характеристику преступления, выделяется каждым криминалистом, независимо от того, какую научную школу он представляет, остановимся именно на этом элементе более подробно.

Следует учитывать, что данный элемент не однороден по своей структуре. Определение способа совершения преступления, появившееся в 70-х гг. прошлого столетия[2], как совокупности действий по подготовке, совершению и сокрытию преступления, так или иначе оспаривалось ведущими криминалистами в части сокрытия следов преступления. Но такая составляющая способа как подготовка

---

[1] *Колесниченко А. Н.* Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. ... докт. юрид. наук. Харьков, 1967. С. 10,14.

[2] *Зуйков Г. Г.* Установления способа совершения преступления. М., 1970. С. 15.

к совершению, естественно умышленных преступлений, молчаливо была принята всеми.

Итак, способ совершения преступления – неотъемлемый элемент криминалистической характеристики преступлений, входящий в структуру любой частной криминалистической методики, не является исключением и методика расследования компьютерных преступлений.

Учитывая множество проведенных исследований, затрагивавших проблемы способов совершения компьютерных преступлений, остановимся лишь на особенностях подготовки к совершению преступлений, предметом преступного посягательства которых является компьютерная информация, передаваемая посредством электронной почты. Тем более что на сегодняшний день невозможно представить организацию, которая бы не обменивалась информацией с другими организациями или учреждениями без использования почтовых серверов.

Способ совершения преступления, в том числе и подготовка к его совершению, практически всегда определяется спецификой деятельности, в области которой планируется совершить преступление.

В наше время глобального развития информационных технологий работа во Всемирной паутине для абсолютного большинства организаций и частных лиц является повседневной необходимостью. Но не все осознают, что кроме современных возможностей Интернет таит в себе и различные угрозы, в частности угрозу безопасности корпоративных данных при несанкционированном удаленном доступе к информационной системе пользователя. Недостаточная защищенность компьютеров или целой сети может привести к искажению информации, заражению вирусами, коллапсу трафика или обеспечить «лазейки» хакерам. Итогом легкомысленного отношения к проблеме безопасности может стать не только искажение информации, но и ее полное уничтожение. Алгоритм работы программных закладок, устанавливаемых на компьютере и передающих данные злоумышленнику, в настоящее время хорошо известен. Тем не менее, иногда проходят недели, прежде чем это выяснится. Задачей, которую приходится решать сетевым администраторам, является выявление рассылок спама и почтовых «бомб» пользователями. Очень часто спамерские программы напрямую подключаются к почтовому серверу жертвы или промежуточному серверу, который является open relay, что затрудняет выявление таких попыток на локальном почтовом сервере. На маршрутизаторе, с использованием ряда программ пакетной фильтрации (например,

IP Filter), с помощью специального правила все SMTP-соединения будут перенаправляться к локальному почтовому серверу. Если этот сервер правильно сконфигурирован, он будет фиксировать все почтовые сообщения и протоколировать все соединения. Для повышения эффективности процесса чаще всего разрешается доверенным хостам обходить этот прокси. После этого достаточно только запустить программу просмотра логов почтового сервера (записей о событиях), чтобы выявить злоупотребления почтой. Такая программа должна периодически просматривать логи, а в случае наличия признаков злоупотреблений уведомлять системных администраторов по электронной почте и блокировать доступ нарушителя к почтовому серверу.

Бывают ситуации, когда почтовый сервер должен принимать письма от неограниченного числа респондентов. В таких ситуациях обычно используются два способа. Первый способ основан на том факте, что легальный пользователь также забирает почту по протоколу POP3 с этого сервера, а следовательно, имеет имя и пароль – POP before SMT. При этом способе пользователь должен сначала забрать почту, после чего на некоторое время (до 15 минут) IP-адрес, с которого он забирал почту, попадает в список адресов, и с него можно будет отправлять письма через данный почтовый сервер. Другой способ – SMTP AUTH (его поддерживают большинство почтовых клиентов). При его использовании пользователь перед началом отправки почты активизируется с помощью специального подпротокола в SMTP. При этом имя и пароль берутся из файла паролей POP3. В таком случае имена спамеров протоколируются перед проверкой домена и IP отправителя.

Поводя итог вышесказанному, подготовку к совершению компьютерного преступления можно представить в виде следующего алгоритма действий:

– получение информации о сетевых технологиях;

– получение данных о способах защиты информации;

– получение информации о закладках, имеющихся в наиболее используемых операционных системах;

– подбор или создание программного обеспечения для взлома защиты (программ подбора паролей, адресов и дешифраторов);

– приобретение или подбор необходимого оборудования.

После чего осуществляется комплекс действий, который с точки зрения криминалистики расценивается как непосредственное совершение преступления.

Основные направления развития криминалистических знаний в условиях информационного общества

Ю. В. Гаврилин,
профессор кафедры,
доктор юридических наук, доцент
(Академия управления МВД России)

В статье рассматриваются направления развития частных криминалистических теорий и учений в условиях цифровизации. Представлены тенденции развития теории идентификации, теории криминалистического прогнозирования, учения о следах, криминалистической тактики и методики расследования отдельных видов преступлений.

Криминалистические знания, цифровизация, электронный образ, электронный след.

В современных условиях криминалистика столкнулась с рядом вызовов и угроз, таких как цифровизация способов подготовки, совершения и сокрытия преступлений, увеличение числа преступлений, совершенных дистанционным способом, использование криптовалют в криминальных взаиморасчетах, рост трансграничной преступности и др.

Данные условия придают колоссальный импульс развитию криминалистики. И это развитие, как представляется, осуществляется в двух направлениях.

Первое направление – актуализация существующих и разработка новых криминалистических технологий выявления, раскрытия, расследования и предупреждения преступлений, то есть в направлении совершенствования криминалистической деятельности в условиях информационного общества.

Второе направление состоит в развитии криминалистических знаний, а также совершенствовании уголовно-процессуальной формы их применения, чему, собственно, и посвящен мой доклад.

В связи с этим следует констатировать, что сложившаяся в конце 50-х гг. прошлого века система науки криминалистики сегодня претерпевает существенную трансформацию за счет формирования новых подразделов криминалистической техники, тактики и методики расследования отдельных видов преступлений, а также развития существующих и формирования новых частных криминалистических теорий и учений.

Основные направления подобной трансформации следующие.

Теория криминалистической идентификации, как фундамент всей науки криминалистики, является одной из наиболее разработанных. Еще с 60-х гг. прошлого века аксиомой считается существование 4-х видов криминалистической идентификации: по материально-фиксированным отображениям признаков; по признакам общего происхождения (целого по частям); по описанию признаков; по мысленному образу.

При этом решение таких экспертных задач, как определение взаимного соответствия информации, содержащейся на различных электронных носителях, или определение наличия на электронном носителе информации с заданными характеристиками, не представляется возможным отнести ни к одному из обозначенных выше видов криминалистической идентификации.

В связи с этим имеются основания утверждать о наличии пятого вида идентификации – *идентификации по электронному образу объекта.*

Отличие данного вида от ранее указанных состоит в особых физических свойствах идентифицируемого (искомого) и идентифицирующего (проверяемого) объектов, особом (специфичном) наборе идентифицирующих признаков, самостоятельной методической и инструментальной базе подобных исследований.

Развитие **теории криминалистического прогнозирования** должно следовать в направлении развития возможностей прогнозирования реализации механизма совершения единичного, конкретного противоправного деяния. В основе подобного прогнозирования должны находиться, в первую очередь, закономерности предкриминального поведения субъекта преступления как элемента механизма его совершения.

При этом цифровизация пополняет инструментарий криминалистики новыми технологиями, уже доказавшими свою эффективность. Вот лишь некоторые из них:

– метод систематизации информации в сети Интернет посредством семантических фильтров;

– мониторинг открытых ресурсов сети Интернет для обнаружения и предупреждения информационных атак специализированными центрами на объектах критической информационной инфраструктуры в рамках государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[1].

[1] Ст. 6 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

Указанные методы способны придать теории криминалистического прогнозирования «второе дыхание», обеспечивая целенаправленную деятельность органов предварительного расследования, дознания и их должностных лиц по выявлению признаков подготавливаемых преступлений.

Развитие **криминалистического учения о следах** обусловлено тем, что следы преступлений, совершенных с использованием информационно-коммуникационных технологий, требуют разработки принципиально иных методов, средств и технологий их обнаружения, фиксации и изъятия, поскольку они, в силу их специфики, носят информационный характер, отражая вызванное расследуемым событием изменение информации, а не ее носителей, то есть материальных объектов.

Вот лишь некоторый перечень следов, позволяющих установить лицо, совершившее преступление с использованием информационно-коммуникационных технологий: IP-адрес компьютера в сети, MAC-адрес сетевого оборудования, адрес электронной почты, идентификатор социальной сети, номер банковской карты, произведенные с ней транзакции, номер телефона, информация о соединениях абонента, информация базовых станций мобильной связи, данные систем геолокации и т. п.

Очевидно, что перечисленные следы не рассматриваются в рамках трасологии, поскольку при их образовании не происходит контактного взаимодействия следообразующего и следовоспринимающего объектов, а само следообразование происходит в результате тех или иных изменений в компьютерной информации путем ее создания, уничтожения, модификации, копирования, блокирования[1].

Сущность данных следов состоит в том, что они, оставаясь на электронных носителях информации, отражают изменения в хранящейся в них информации по сравнению с исходным состоянием.

Соответственно, криминалистическое учение о следах получает свое развитие, разрабатывая технологию работы с данной категорией криминалистических объектов.

Развитие **учения о криминалистической регистрации** обусловлено изменениями объектов учета, системы регистрации, способов ведения учетов, внедрением новых видов автоматизированных информационно-поисковых систем, совершенствованием технологии получения информации (из различных источников), необходимой для принятия субъектами расследования процессуальных, так-

[1] *Гаврилин Ю.В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 25. С. 3.

тических, организационных решений. В качестве положительного примера можно привести работу подразделений ГУ МВД России по Саратовской области, где активно применяется автоматизированная система учета абонентских номеров, IP-адресов, IMEI-телефонов (регистрация и ведение учета осуществляется по номеру регистрации сообщений о преступлении (КУСП). Вместе с тем, на федеральном уровне подобной системы до нестоящего времени нет.

Представляется, что централизованная постановка на учет похищенных номерных вещей IMEI-номеров похищенных телефонных аппаратов совместно с внесением изменений в ФЗ «О связи» о возложении на операторов связи обязанности по блокировке оборудования, находящегося на учете похищенного имущества, существенно сократила бы такой вид криминального бизнеса, как хищения сотовых телефонов.

Как уже отмечалось, обнаружение, фиксация и изъятие электронных следов преступления требует использования особых криминалистических технологий[1], разработка и совершенствование которых на протяжении уже ряда лет представляют исключительно актуальное направление криминалистики. Сказанное предопределяет появление самостоятельного подраздела криминалистической техники – **криминалистического исследования электронных носителей информации**, направленного на обеспечение единообразного подхода к работе с данными объектами. К числу последних следует отнести любые устройства, конструктивно предназначенные для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

К числу объектов криминалистического исследования электронных носителей информации, вне всякого сомнения, относятся и средства подвижной радиотелефонной (мобильной) связи с доступом в сеть Интернет (смартфоны) и иные информационно-коммуникационные устройства, включая планшетные компьютеры. В связи с наличием в абсолютном большинстве современных смартфонов модуля получения геопространственной информации, использующего сигналы систем ГЛОНАСС и (или) GPS-навигации, перспективным направлением развития выше-

[1] *Гаврилин Ю. В., Лыткин Н.Н.* Использование компьютерно-технических следов при установлении события преступления // Известия Тульского государственного университета. Серия: актуальные проблемы юридических наук. Вып. 15. Тула, 2006. С. 44–50.; *Гаврилин Ю.В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 23. С. 2–5; и др.

названного подраздела криминалистической техники является и исследование данных средств навигации[1].

Помимо перечисленного, к числу объектов криминалистического исследования электронных носителей информации относятся: системы обработки информации или отдельные функциональные устройства таких систем; системные блоки персональных компьютеров, ноутбуков, нетбуков и т. п; машинные носители (накопители на жестких и гибких магнитных дисках, флеш-накопители, карты памяти, оптические диски и т. п.); уже упомянутые навигаторы, трекеры; мобильные телефоны и сим-карты к ним; радиоэлектронные устройства; платежные пластиковые карты и скимминговые устройства[2]; платы игровых автоматов; видеорегистраторы и прочее. При этом расширение спектра объектов криминалистического исследования электронных носителей информации сопровождается развитием средств извлечения криминалистически значимой информации из устройств мобильной связи, в частности «Cellebrite UFED», «Мобильный криминалист», «Belkasoft Evidence Center Ultimate», «Elcomsoft Mobile Forensic Bundle» и др.

Активно развивающиеся в настоящее время технологии искусственного интеллекта, анализа больших объемов данных способны найти отражение в развитии **учения о планировании расследования преступлений.** В литературе получило освещение использование методов искусственного интеллекта при изучении личности серийных убийц. При этом была создана самообучаемая нейронная сеть, использующая определенные характеристики известных серийных убийц, включая их биологические, социальные и психологические параметры[3]. Разрабатываются и внедряются в практическую деятельность экспертные правовые системы поддержки принятия решений. Такие системы уже находят свое практическое применение при расследовании хищений в строительстве, рас-

---

[1] *Гаврилин Ю.В.* Использование возможностей средств навигации в установлении обстоятельств совершения преступлений // Актуальные проблемы борьбы с преступностью: материалы межвузовской науч.-практ. конф. (Тула, 15 марта 2017 г.) / Тул. ин-т (филиал) ВГУЮ (РПА Минюста России). Тула: Тул. ин-т (филиал) ВГУЮ (РПА Минюста России), 2017.

[2] Под скиммером понимается специальная накладка на стандартные органы управления банкомата (картоприемник, клавиатура), обеспечивающая фиксацию сведений, содержащихся на магнитной полосе карты и введенного с клавиатуры ПИН-кода, снабженные функцией трансляции полученной информации по радиоканалу или фиксации полученных данных на встроенный электронный носитель.

[3] *Ясницкий Л. Н., Валуева С. В., Сафонова Д. Н., Черепанов Ф.М.* Использование методов искусственного интеллекта в изучении личности серийных убийц // Всероссийский криминологический журнал. 2015. № 3. С. 423–430.

следовании преступлений в сфере безопасности движения и эксплуатации транспорта и др[1]. Развиваются системы компьютерного моделирования при планировании расследования преступлений[2], а также программные средства управления проектами. Последнее направление представляется особенно актуальным, поскольку позволяет с использованием диаграмм Ганта визуализировать структуру перечня следственных действий, иных процессуальных и непроцессуальных мероприятий, а также контролировать своевременность завершения запланированных мероприятий на определенный момент времени. Это позволяет использовать программы управления проектами не только для планирования расследования преступлений, но и для осуществления процессуального контроля за соблюдением сроков расследования, избрания меры пресечения в досудебном судопроизводстве.

Не вызывает сомнений обоснованность формирования такого подраздела криминалистической тактики, как **получение доказательственной информации на электронных носителях.** Данный подраздел, как представляется, сможет включать научные положения и основанные на них рекомендации по проведению отдельных следственных и иных процессуальных действий, направленных на формирование доказательств на электронных носителях и их использование в процессе доказывания по уголовному делу.

При этом следует выделить два направления развития криминалистических знаний.

Первое. Создание правовых оснований возникновения доказательственной информации. В настоящее время правовые основания возникновения доказательственной информации по уголовным делам о преступлениях, совершенных с использованием информационных и коммуникационных технологий, содержатся в весьма широком массиве нормативно-правовых актов различного уровня.

Так, получение информации о движении денежных средств на счетах конкретных лиц мы получаем на основании ст. 26 Закона РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности».

Обязанность операторов связи хранить весь передаваемый абонентами контент (СМС, ММС, голосовые сообщения, сообще-

---

[1] *Баранов С.А.* Информационные технологии в юридической деятельности: учеб. пособие / С.А. Баранов, Ю.Э. Голодков, В.И. Демаков, Е.Ю. Ларионова, Е.Е. Кургалеева. Иркутск: ФГКОУ ВО ВСИ МВД России, 2015. С. 191–198.

[2] *Ковалев С.А., Смагоринский Б.П.* Использование криминалистического компьютерного моделирования при планировании расследования преступлений // Юридическая наука и правоохранительная практика. 2013. № 4 (26). С. 111–123.

ния мессенджеров) регламентируется ст. 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи».

Обязанность провайдеров идентифицировать пользователей при предоставлении доступа в сеть Интернет установлена ст. 10.1 Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защиты информации».

Контроль за онлайн-платежами предусмотрен ст. 7 Федерального закона РФ от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Запрет на использование анонимайзеров установлен ст. 15.8. Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защиты информации».

Это лишь несколько примеров, показывающих, как отраслевое законодательство предоставляет субъектам расследования дополнительный правовой инструментарий собирания доказательственной информации. Следует заметить, что такая ситуация имеет место в любой сфере, регулируемой техническими нормами и правилами (транспорт, связь, строительство, энергетика и т. д.).

Второе. Совершенствование процессуальных средств получения доказательственной информации.

Совершенствование технологической основы **учения о фиксации доказательственной информации** осуществляется за счет таких новых технологий, как:

– преобразование речевой информации в письменную;

– привязка местонахождения объекта к геопространственным координатам;

– определение расстояния между объектами с использованием лазерных дальномеров;

– технология дублирования содержимого электронных носителей в процессе копирования и др.

Вместе с тем, довольно широкую дискуссию в уголовно-процессуальной науке вызывает вопрос относительно возможности и порядка использования технологии блокчейн для целей фиксации доказательственной информации.

Не пытаясь оценивать достоинства и недостатки подобной технологии применительно к хранению относительно большого объема материалов уголовных дел, следует отметить несомненную ценность процессуальной письменной формы как фундаментальной гарантии соблюдения прав всех участников судопроизводства. В связи с этим представляется преждевременным осуществление отказа от письменной формы уголовного судопроизводства на досудебных стади-

ях, призывы к которому возникают в литературе. До тех пор, пока уровень проникновения цифровых технологий не позволит полностью заменить собственноручную подпись документов каждым участником уголовного процесса, полный переход с письменной формы на цифровую не представляется возможным, что не исключает при этом цифровизацию отдельных процессуальных действий: направление и получение запросов, поручений, справок и т. п.

Вектором развития **методики расследования отдельных видов преступлений** является переработка и дополнение частных криминалистических методик, построенных без учета электронных следов преступлений.

В основе такой переработки должны лежать универсальные алгоритмы решения таких типичных тактических задач, как установление события преступления в цифровой среде; установление лица, совершившего преступление, по оставленным им электронным следам: IP-адресу, MAC-адресу, адресу электронной почты, идентификатору социальной сети, номеру банковской карты, номеру телефона, информации о соединениях абонента, произведенных транзакциях и т. п.; установление ущерба и обеспечение его возмещения; установление обстоятельств совершения преступления; доказывание виновности лица в совершении преступления; установление причин и условий совершения преступления и пр.

Таким образом, ответом науки криминалистики на вызовы и угрозы современности является интеграция в существующие криминалистические учения и теории современных информационных технологий, а также структурные преобразования, рассмотренные выше.

Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемым с использованием информационных технологий

В. В. Гончар,
доцент кафедры,
кандидат юридических наук
(Московский университет МВД России
им. В.Я. Кикотя)

Предлагаемая статья посвящена отдельным аспектам совершенствования подготовки сотрудников правоохранительных органов. Особое внимание уделяется проблемам подготовки по противодействию преступлениям, совершаемым с использованием информационных технологий.

Уголовная политика, уголовно-процессуальная политика, уголовно-процессуальное законодательство, проблемы уголовного судопроизводства, противодействие компьютерным преступлениям, расследование преступлений, совершаемых с использованием информационных технологий.

Президент Российской Федерации В. В. Путин 1 декабря 2016 г. в Послании Федеральному Собранию РФ определил следующее: «Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Предлагаю запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики. В ее реализации будем опираться именно на российские компании, научные, исследовательские и инжиниринговые центры страны. **Это вопрос** национальной безопасности и технологической независимости России, в полном смысле этого слова – **нашего будущего** (выделено авт.)»[1].

28 февраля 2018 г., выступая на расширенном заседании коллегии МВД России, В. В. Путин отметил низкий уровень раскрывае-

[1] URL:https://infoforum.ru/conference/conference/program/cid/32 (дата обращения: 28.02.2018).

мости преступлений против собственности, совершаемых с использованием компьютерных и телекоммуникационных технологий[1].

Поставленные Президентом России вопросы не только актуальны, но и достаточно сложны, поскольку существующая ситуация свидетельствует о значительных изъянах в системе защиты населения и государственных институтов от киберугроз. Криминально ориентированные лица все более активно осваивают новые технологии и наращивают криминальную активность в виртуальном пространстве, в том числе в его экономическом сегменте. Об этом, в частности, сообщил председатель правления ПАО «Сбербанк России» Г.О. Грефф, по данным которого «98,5 % преступлений, совершенных в финансовой сфере, это киберпреступления, а оставшиеся 1,5 % это традиционные способы совершения подобных преступлений...».[2]

Анализируя сложившуюся ситуацию в информационной среде, возможно выделить следующие проблемы обеспечения кибербезопасности в России:

1) действующая государственная система обеспечения безопасности и противодействия киберугрозам не вполне эффективна, в том числе и потому, что принимаемые меры по «улучшению, усилению и углублению» нередко остаются «декларацией о намерениях» и не дают ожидаемого результата;

2) отсутствует эффеективное взаимодействие государства и общества в области кибербезопасности. Не сформирована система оперативного обмена информацией с бизнесом (например, с представителями финансово-кредитных учреждений, сотовых операторов, интернет-провайдеров), хотя это объективно необходимо для успешного противодействия настоящим и будущим киберугрозам;

3) государственные органы – регуляторы, в основном занимающиеся надзорными функциями, недостаточно участвуют в создании системы киберзащиты. Не всегда эффективно применяется риск-ориентированный подход при создании требований по информационной защите в принимаемых нормативных актах;

4) на уровне государства разработана (в 2000 г.) и существенно обновлена (в конце 2016 г.) Доктрина информационной безопасно-

---

[1] См: Информация о расширенном заседании коллегии МВД России // URL:http://kremlin.ru/events/president/news/56949 (дата обращения: 28.02.2018).

[2] См: Пресс-конференция «Сбербанк делится знаниями: образовательные проекты Банка», проходившая в Информационном агентстве России ТАСС 25 января 2017 г. // URL: https://xn--l1aeji.xn--b1aew.xn--p1ai/Press-sluzhba/Novosti/ item/ 9330529/ (дата обращения: 28.02.2018).

сти, однако отсутствуют механизмы ее реализации, сопоставимые с масштабами киберугроз, существующими в настоящее время;

5) принципы осуществления оперативной работы, предварительного следствия (дознания), судебного разбирательства в основном унаследованы из «прошлого века», когда они обеспечивали вполне успешное противодействие традиционной преступности. Однако в настоящее время данные правоохранительные механизмы не всегда обеспечивают успешное противодействие современной высокотехнологичной преступности. Кроме того, не в полной мере сформирована система государственных учреждений, производящих компьютерно-технические и иные судебные экспертизы по уголовным делам о преступлениях, совершаемых с использованием информационных технологий;

6) недостаточно совершенно законодательство в области противодействия киберпресуплениям (например, не установлена уголовная ответственность за фишинг (компьютерные преступления, основанные на принципах социального инжиниринга) и рассылку вредоносного спама, как за отдельный вид преступлений);

7) система подготовки юридических и технических кадров не вполне соответствует существующим угрозам;

8) невысокая компьютерная грамотность и осведомленность о современных киберугрозах большинства населения и управленцев различных уровней в России создает благоприятную среду для киберпреступников, совершающих противоправные деяния в самом широком спектре общественных отношений в масштабах, угрожающих национальной безопасности.

Анализируя варианты противодействия и преодоления данной, мягко говоря, «непростой» ситуации, необходимо отметить, что это должны быть не фрагментарные усилия по реагированию на отдельные виды киберугроз (атаки на банк, аэропорт, отдельные информационные ресурсы и т. п.), а самостоятельное направление государственной политики, основанное на Указе Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[1], в п. 18 которой указано: «Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок ***и недостаточным кадровым обеспечением в обла-***

[1] URL: http:// www.pravo.gov.ru (дата обращения: 25.04.2018).

сти информационной безопасности (выделено авт.), а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом ***мероприятия*** (выделено авт.) по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую ***не имеют комплексной основы*** (выделено авт.).

Следовательно, основой государственной политики в области информационной безопасности является обучение и воспитание соответствующих кадров, которые бы обеспечили «прорывные» результаты в области информационной безопасности России.

Данный подход предусматривает необходимость существенных изменений как в структуре, так и в организации учебного процесса в образовательных учреждениях, особенно в вузах, организующих подготовку специалистов в области информационной безопасности. К данной категории специалистов, наряду со специалистами технических профилей, безусловно относятся сотрудники правоохранительных органов (сотрудники оперативных подразделений, дознаватели, следователи, прокуроры, судьи).

По нашему мнению, достаточно быстрый и положительный результат может дать взаимодействие вузов с организациями, имеющими определенные достижения в области обеспечения собственной информационной безопасности. Одними из ключевых субъектов в данной сфере деятельности, безусловно, являются ПАО «Сбербанк России», «Лаборатория Касперского» и некоторые другие организации.

По нашему мнению, для совершенствования подготовки в вузах, сотрудников правоохранительных органов, специализирующихся на раскрытии и расследовании преступлений в сфере информационных технологий, целесообразно сформировать отдельные структуры, например**:**

– ***научно-исследовательскую группу***, сотрудники которой имели бы достаточно возможностей по изучению и разработке проблем, связанным с расследованием преступлений в сфере информационных технологий;

– ***координирующую группу***, сотрудники которой смогут заниматься организацией взаимодействия вуза с представителями иных вузов, организаций и учреждений;

– ***экспертно-консультативную группу***, сотрудники которой будут контролировать, проверять и осуществлять приемку резуль-

татов работ научно-исследовательской и контрольно-координирующей групп.

В заключение следует отметить, что подобные группы необходимо сформировать не только в профильных вузах и организациях, разрабатывающих вопросы кибербезопасности, но и в государственных органах, имеющих отношение к профилактике, предотвращению, раскрытию и расследованию киберпреступлений.

Общество стремительно движется к цифровому будущему и проблемы обеспечения безопасности такого будущего станут все более актуальны. Без подготовки квалифицированных правоохранительных кадров, способных обеспечить должный уровень информационной безопасности, эти проблемы невозможно будет успешно разрешить.

Криминалистическое обеспечение раскрытия и расследования хищений денежных средств, выделяемых на реализацию приоритетных направлений развития сельского хозяйства

О. П. Грибунов,
заместитель начальника,
доктор юридических наук, доцент
(Восточно-Сибирский институт МВД России)

Учитывая роль и значение государственной поддержки развития агропромышленного комплекса, в статье обосновывается необходимость криминалистического обеспечения раскрытия и расследования хищений денежных средств, выделяемых на реализацию приоритетных направлений развития сельского хозяйства.

Агропромышленный комплекс, приоритетные направления развития, криминалистический анализ, криминалистическое обеспечение.

Начиная с 2005 г. приоритетные направления развития отраслей экономики становятся объектом пристального внимания со стороны государства, когда были впервые нормативно обозначены и урегулированы приоритеты государственной социально-экономической политики, а именно агропромышленный комплекс, здравоохранение, образование и жилищная сфера. Реализация мероприятий по финансовому обеспечению данных отраслей осуществляется как в рамках приоритетных национальных проектов, так и государственных программ. Но если здравоохранение, образование и жилищная сфера имеют ярко выраженный социальный окрас и их роль и предназначение в обеспечении благополучия населения вполне очевидна, то для экономики особое значение имеет развитие агропромышленного комплекса (АПК).

Безусловно, учитывая международную ситуацию, следует отметить, что в аграрном секторе экономики происходят колоссальные экономические преобразования. Одна из проблем, которая неизбежно возникает в условиях экономического кризиса, это процесс криминализации отраслей народного хозяйства и экономики. В том числе такому процессу подвержен и агропромышленный комплекс[1].

[1] *Янин С. А.* К вопросу об организации расследования преступлений в сфере агропромышленного комплекса / С. А. Янин // Юридическая наука и правоохранительная практика. 2016. № 4 (38). С. 168.

Некоторые исследования показали, что данная сфера производства имеет одни из самых высоких показателей криминализованности. Это принято связывать со значительной финансовой поддержкой этого направления экономической деятельности[1].

Только за последние 5 лет на развитие АПК было направлено более 1,2 трлн рублей[2], что требует тщательного контроля за их точным и неукоснительным исполнением, так как неэффективное и нецелевое использование данных средств оказывает негативное влияние на экономическую безопасность государства. Это колоссальные средства, объем которых в совокупности с государственным характером их принадлежности сказывается на характеристике преступных посягательств. Особенно это влияет на характер способа совершения преступлений и личность преступников.

Анализ статистических данных позволяет заключить, что несмотря на определенную положительную тенденцию к снижению преступлений в данной отрасли, размер причиненного ущерба остается колоссальным. Кроме того, для таких преступлений характерна высокая степень латентности. Так, по официальным данным ГИАЦ МВД России, в 2015 г. выявлено 429 (-21,6 %) преступлений в сфере реализации приоритетных направлений развития сельского хозяйства, причинивших материальный ущерб в размере 3 227 313 тыс. рублей, выявлено 290 (-11,3 %) лиц, виновных в совершении указанных преступлений, в 2016 г. – 332 (-22,86 %) преступлений, причиненный ими размер материального ущерба составил 1 115 518 тыс. руб., выявлено 215 (-25,9 %) лиц, в 2017 г. – 228 (-31,3 %) преступлений, 283 287 тыс. рублей – ущерб, выявлено 130 (-39,5%) лиц, соответственно[3].

Состояние аграрного сектора прямо отражается на состоянии безопасности в сфере экономики и продовольственного положения. Меры по повышению экономической безопасности в настоящее время должны быть направлены на обеспечение состояния защищенности отдельных направлений финансовой поддержки со стороны государства основных отраслей народного хозяйства. Экономическая безопасность в целом и отдельные аспекты ее состояния в определенной мере подвержены негативному влиянию.

---

[1] *Репин М.Е.* Характеристика преступлений мошеннического характера, совершаемых в сфере агропромышленного комплекса / М. Е. Репин // Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 178.

[2] *Медведев Д.А.* Отчет Правительства о результатах работы в 2012–2017 годах // Рос. газ. 2018. № 77 (7540). 12 апр.

[3] Официальный сайт ФКУ ГИАЦ МВД России [Электронный ресурс]. URL: http://10.5.0.17/csi/modules/ (дата обращения: 11.02.2018).

Важным звеном в обеспечении экономической безопасности реализации приоритетных направлений развития сельского хозяйства является контроль за выделенными средствами. Немаловажную роль в обеспечении целевого поступления выделенных государством бюджетных средств играют органы внутренних дел, соответствующие подразделения которых проводят комплекс оперативно-розыскных мероприятий по выявлению и пресечению фактов мошенничества, хищений и нецелевого использования бюджетных средств, выделяемых на реализацию поддержки основных отраслей народного хозяйства и государственных программ.

В ряде направлений аграрной политики преступные посягательства на выделяемые для их реализации средства имеют особенно широкое распространение. Это достаточно хорошо заметно при анализе судебной и следственной практики по преступлениям изучаемой категории. Именно они требуют внимания и тщательного криминалистического изучения. Так, в контексте криминалистической профилактики необходимо выделить следующие направления аграрной политики, обладающие криминалистически значимой информацией: во-первых, это комплекс мер, направленных на расширение кредитования сельскохозяйственной деятельности и придания процессу получения кредита более доступного характера; во-вторых, это меры, заключающиеся в широком распространении субсидирования со стороны государства различных экономических процессов в деятельности сельхозпроизводителей и в социальной сфере жизни села. Как показал анализ судебной и следственной практики по преступлениям изучаемой категории, именно в этих направлениях стимулирования аграрного сектора экономики происходит наибольшее число хищений и сопутствующих им преступлений.

Соответственно, речь идет как о должностных преступлениях в сфере экономики, так и преступлениях, совершенных лицами, выполняющими управленческие функции в коммерческих и иных организациях, которые на должном уровне исследованы А. В. Варданяном и К. В. Гончаровым[1]. При этом каждое направление имеет

[1] *Варданян А. В., Гончаров К. В.* Общие положения допроса свидетелей и потерпевших по делам о злоупотреблениях полномочиями лицами, выполняющими управленческие функции в коммерческих и иных организациях / А. В. Варданян, К. В. Гончаров // Общество и право. 2017. № 3 (61). С. 130–134; *Варданян А. В., Гончаров К. В.* Злоупотребление управленческими полномочиями в коммерческой или иной организации: опыт правоприменительной практики и некоторые проблемы возбуждения уголовного дела и предварительного расследования / А. В. Варданян, К. В. Гончаров // Юристъ–Правоведъ. 2015. № 2 (69). С. 49–52; *Варданян А. В., Гончаров К. В.* Механизм злоупотре-

потребность в «формировании комплексной методики расследования экономических преступлений в сфере служебной деятельности как частной криминалистической методики расследования преступлений высокой степени общности»[1].

Все вышеизложенное позволяет констатировать, что приоритетные направления развития сельского хозяйства в силу своей специфики относительно обстановки их реализации и субъектов деятельности все чаще становятся объектом преступных посягательств с высокой степенью латентности, и криминалистическое обеспечение деятельности правоохранительных органов по декриминализации данной сферы заслуживает самостоятельного изучения как объект криминалистического исследования.

бления полномочиями субъектами управленческих функций в коммерческих и иных организациях как методологическая основа для формирования частной криминалистической методики расследования преступлений / А. В. Варданян, К. В. Гончаров // Известия Тульского государственного университета. Экономические и юридические науки. 2015. № 4–2. С. 3–9.

[1] *Варданян А. В., Айвазова О.В.* Должностные преступления в сфере экономики как объект криминалистического научного анализа / А. В. Варданян, О. В. Айвазова // Труды Академии управления МВД России. 2017. № 1 (41). С. 72.

Мошеннические риски в сфере создания форков криптовалют и первичного размещения монет (ico)

П. В. Гридюшко,
начальник кафедры,
кандидат юридических наук, доцент
(Академия МВД Республики Беларусь)

В статье рассматриваются проблемы совершения мошенничеств и возможности их выявления при создании новых криптовалют и проведения первичного размещения монет.

Мошенничество, риски, форки, криптовалюта, первичное размещение монет.

Прошедший 2017-й и завершающийся 2018-й г. характеризуются повышенным ажиотажем вокруг новомодных категорий «блокчейн», «криптовалюта», «ICO» и т. п. Этот массовый интерес был сформирован резким взлетом курса криптовалют по отношению к фиатным деньгам, особенно когда в декабре 2017 г. биткоин преодолел отметку в 20 000 долларов (высокий прирост показывали и иные альткоины). Последующая коррекция и падение курсов не охладили сформировавшийся интерес, а лишь подогревали его, подкрепляя рядом различных рассуждений, что после роста всегда идет коррекция, а затем опять рост.

Подавляющее большинство населения не в полной мере понимает принципы существования блокчейна, особенности функционирования криптовалют и т. д., но с восторгом воспринимает новости об очередном разбогатевшем студенте, который несколько лет назад, вложив в криптовалюту 10–20 долларов, благодаря росту курса стал миллионером. Естественно, каждый в глубине души желает повторить этот путь. При этом внимание общества привлекают как состоявшиеся криптовалюты (Bitcoin, Ethereum, Ripple, Litecoin, Dash, Nem и др.), так и только появляющиеся.

В данном контексте очевидно, что желание быстро разбогатеть фактически ничем не рискуя реализуется большинством граждан путем поиска «нового биткоина» или «нового эфириума», т. е. криптовалюты, только выходящей на биржу и стоящей очень дешево (не каждый может себе позволить пойти на риск и вложить крупные денежные суммы в тот же самый биткоин, который даже если и вырастет в два раза, то прибыль составит «лишь» 100 %). Ожида-

ние последующего роста на сотни, а то и на тысячи процентов именно новых криптовалют превалирует над рисками потерять вложенные инвестиции. Тем более что в случае с новыми альткоинами эти инвестиции для одного отдельно взятого человека не так уж и велики (в этом – то и состоит главная цель таких инвесторов – получить прибыль, рискуя относительно небольшими денежными суммами). Понимая основы психологии толпы, работая на поддерживаемом, в том числе и средствами массовой информации, ажиотаже, в мире ежедневно появляются десятки новых криптовалют, которые активно предлагаются населению.

Общая идея децентрализованной валюты, заложенная в 2009 г. человеком (или группой людей) под псевдонимом СатошиНакамото, сама по себе является достаточно интересной (ограниченная эмиссия, быстрые переводы денег без посредников и т. д.). Когда на рынке начали активно появляться новые криптовалюты, их разработчики старались предусмотреть новые возможности (технология смарт-контрактов – Ethereum, анонимность – Dash, Monero, увеличенная скорость транзакций – Ripple, Litecoin и т. д.). Для того чтобы криптовалюта стала популярной, необходимы какие-то существенные новшества. Однако далеко не всегда подобные новшества наблюдаются.

Отчасти этому способствует открытый исходный код биткоина, который позволяет создать свою «новую» криптовалюту (счет таких ответвлений уже идет на тысячи). В данном случае созданный альткоин в принципе по своему функционалу ничем отличаться от биткоина не будет. Однако создание сайта, новое название криптовалюты, активная рекламная кампания позволяют обратить на данный продукт внимание общественности. Схема обогащения «разработчиков» довольно проста:

1) до проведения рекламной кампании осуществить премайнинг (так как на первых этапах сложность вычислений достаточно низкая);

2) продолжая рекламировать новую криптовалюту, надеяться на повышенный общественный интерес;

3) при наступлении такого, физические и юридические лица начинают инвестировать в данный продукт. Естественно, повышенный спрос поднимает цену криптовалюты;

4) при возросшем курсе – разработчики продают все свои монеты (полученные в ходе премайнинга). Данный ход обрушит курс и новая криптовалюта благополучно забывается, а потратившие свои сбережения граждане продолжают искать очередную криптовалюту.

Вопрос об усмотрении признаков мошенничества в таких случаях остается открытым. Конечно, в качестве индикаторов могут выступать отсутствие хорошего сайта, мобильных приложений, подробностей о новой монете, команде разработчиков, документации и т. д., однако процесс доказывания по таким фактам будет весьма сложным. При этом сами «инвесторы», как правило, никаких претензий не имеют, поскольку рассматривают вложение своих средств в очередную криптовалюту отчасти как лотерею (есть шанс приумножить свой капитал, как, впрочем, есть шанс и потерять вложенные средства). Излишне говорить, что судебная практика в этой области отсутствует.

Достаточно схожим по своей сути с созданием новой криптовалюты является и ICO («Initialcoinoffering» – первичное размещение монет), являющееся одной из форм привлечения инвестиций в виде продажи инвесторам новой криптовалюты, т. н. токенов. Иногда ICO называют одной из форм краудфандинга (коллективного финансирования какого-либо проекта). Говоря же простым языком, ICO – это выпуск какого-то количества монет или токенов и попытка убедить будущих инвесторов обменять их на более ликвидные монеты, например Bitcoin или Ethereum, по заранее установленному курсу. Как правило, для этих целей используются токены на базе Ethereum, ведь для этого достаточно выпустить смарт-контракт[1].

В целом же, как видно, в основе ICO заложены принципы IPO (первичного публичного предложения акций). А выпускаемые токены очень близки по содержанию к акциям. Неспроста глава американской Комиссии по ценным бумагам и биржам (SEC) Д.Клейтон отметил, что в большинстве случаев токены де-факто являются ценными бумагами, так как их стоимость зависит от деятельности компании, проводящей ICO, к тому же в них можно инвестировать и ими можно торговать для извлечения прибыли. На основании этого он заявил о необходимости регулирования транзакций с токенами и ICO – так же, как регулируются операции с ценными бумагами и IPO[2].

Ряд ICO за последние два года показали впечатляющие результаты для ранних инвесторов, что, естественно, спровоцировало лавинообразный спрос на новые ICO. Согласно веб-сайту

---

[1] ICO: как провести и сколько это стоит? [Электронный ресурс]. Режим доступа: URL: http://polygant.net/ru/ico-sroki-i-stoimost/ (дата обращения: 25.04.2018).

[2] В США поднят вопрос о регулировании криптовалютных бирж и ICO на федеральном уровне [Электронный ресурс]. Режим доступа: URL: https://bitcryptonews.ru/news/ico/v-ssha-podnyat-vopros-o-regulirovanii-kriptovalyutnyix-birzh-i-ico-na-federalnom-urovne (дата обращения: 28.04.2018).

CoinSchedule только за 4 месяца 2018 г. в различные продажи токенов было вложено более 6,5 млрд долларов[1]. Естественно, существует огромное количество попыток злоупотребить текущей рыночной тенденцией путем проведения мошеннических ICO. По разным данным, около 10 % ICO признаются провалившимися, а лишь 8 % впоследствии размещают свои токены на биржах. Мошенническими же являются около 80 % всех проводимых ICO[2]. И примеры наиболее крупных из них постоянно приводятся в том числе и в средствах массовой информации. Так, в апреле 2018 г. во Вьетнаме инвесторы двух предположительно мошеннических ICO закрыли офисы и скрылись в неизвестном направлении. В результате ICO двух стартаповIfan и Pincoin, деятельность которых велась под именем ModernTech, инвесторами было потеряно около 660 млн долларов, пострадали 32 000 инвесторов[3].

В сложившейся ситуации правоохранительным органам нужно быть готовыми к новым вызовам, в том числе с точки зрения не только расследования, но и предупреждения таких фактов. Попытки научиться распознавать мошеннические ICO на ранних этапах его существования предпринимаются учеными из разных стран мира. Например, исследователи из Калифорнийского, Мичиганского и Стэнфордского университетов создали алгоритм, который позволяет обнаружить мошеннические ICO с точностью до 83 %. Они загрузили в систему данные о 2 251 ICO, проведенном с начала 2016 г. Алгоритм сопоставлял продолжительность существования проекта и изменение цен на криптовалюту с информацией об ICO (WhitePaper, информация об учредителях, сайт проекта, социальные сети и другие данные). Отмечается, что разработка позволит инвесторам выявлять мошеннические ICO на раннем этапе[4].

В целом среди наиболее ярких индикаторов, позволяющих заподозрить мошенническое ICO, можно выделить:

1) уверения в гарантированной высокой доходности;

---

[1] CryptocurrencyICOstats 2018 [Электронный ресурс]. Режим доступа: URL: https://www.coinschedule.com/stats.html (дата обращения: 02.05.2018).

[2] См. напр.: Новое исследование: 81 % ICO — скам, только 8 % токенов размещаются на биржах [Электронный ресурс]. Режим доступа: URL: https://bitnovosti.com/2018/03/29/novoe-issledovanie-81-ico-skam-tolko-8-tokenov-razmeshhayutsya-na-birzhah/ (дата обращения: 02.05.2018).

[3] Вьетнам расследует случай мошенничества ICO после заявлений о потерях в $ 660 млн [Электронный ресурс]. Режим доступа: URL: http://chainmedia.ru/news/vietnam-ico-fraud/ (дата обращения: 02.05.2018).

[4] IcoRating: A Deep-Learning System for Scam ICO Identification [Электронныйресурс]. – Режим доступа: https://arxiv.org/pdf/1803.03670.pdf (дата обращения: 04.05.2018).

2) открытые сведения о команде разработчиков (напр., Литовский стартапProdeum, обещавший «привнести блокчейн во фрукты и овощи», после успешного ICO удалил сайт. Перед исчезновением проект продал около 18 % токенов (на общую сумму в полмиллиона долларов, по другим данным – сумма в 10 раз больше). Пользователи заметили, что на сайте Prodeum использовались поддельные фото и персональные данные команды)[1]. Здесь же можно вести речь об отсутствии активности разработчиков в социальных сетях и т. д.;

3) может вызывать сомнение и отсутствие в команде разработчиков специалистов в области продвигаемой идеи (в зависимости от того, какой продукт предлагается: путешествия, логистика и т. д.);

4) излишне агрессивная рекламная кампания, ежедневно рассылающая на электронную почту потенциальных инвесторов новости о новых возможностях и планах проекта. Все планы у качественно подготовленного ICO уже прописаны на первоначальном этапе;

5) внимательное изучение WhitePaper может показать ее скомпилированность из других аналогичных документов, нерациональность составленной сметы расходов, отсутствие сведений о последующей монетизации проекта;

6) отсутствие сведений о характеристиках предлагаемого токена либо такие характеристики не являются уникальными. «Если у него меньше трех функций и его можно заменить обычной криптовалютой, то это тревожный сигнал... Если токен не интегрирован в экономику проекта, то, вероятно, его цель – просто сбор денег... Даже если вся система будет успешной, но токен в ней не играет никакой роли, то не будет никакой мотивации роста его потребления»[2];

8) уверение в том, что проект базируется на технологии блокчейн, когда в этом нет никакой необходимости. Именно с помощью модных терминов «блокчейн», «технология распределенного реестра» инвесторов и широкую аудиторию привлекают к технологиям, в которых они не в полной мере разбираются. Огромное количество появляющихся ICO само по себе вызывает сомнение, что каждое из них является чем-то новаторским. Определить, что проект пытается привлечь инвесторов просто модной терминологией, можно, в том числе и по следующим признакам: если в WhitePaper

---

[1] Блокчейн-стартап Prodeum «пропал» с деньгами инвесторов вскоре после старта ICO [Электронный ресурс]. Режим доступа: URL: https://forklog.com/blokchejn-startap-prodeum-propal-s-dengami-investorov-vskore-posle-starta-ico/ (дата обращения: 04.05.2018).

[2] Как инвесторы выявляют мошеннические ICO [Электронный ресурс]. Режим доступа: URL: https://www.vedomosti.ru/technology/articles/2018/03/06/752836-moshennicheskie-ico (дата обращения: 25.04.2018).

заменить все слова «блокчейн» на «базу данных» и смысл абсолютно не изменится; если проект не децентрализованный, открытый, нейтральный, безграничный, цензуроустойчивый; если проект вместо третьей стороны вводит нового посредника и сам становится посредником.

В завершение следует отметить, что с развитием знаний о выявлении мошеннических ICO повышается и качество их подготовки. Ряд агентств оказывают услуги по их проведению, сопровождению. В сети Интернет существует огромное количество пошаговых инструкций о «запуске» ICO. Так, запрос в поисковике Google «как провести ICO» предлагает 411 000 ответов. И естественно, что правоохранительные органы не должны отставать от последних тенденций в криптовалютном мире.

Использование информационно-коммуникационных технологий в противодействии преступности

Ж. Р. Дильбарханова,
доктор юридических наук, профессор
(Алматинская академия МВД Республики Казахстан им. М. Есбулатова)

В статье анализируются направления использования информационно-коммуникационных технологий в противодействии преступности, оценивается результативность применения конкретных программных продуктов, вносятся предложения о расширении на их базе межгосударственного взаимодействия.

Информационно-коммуникационные технологии, информационные банки данных, борьба с преступностью.

Проблема преступности в современном мире продолжает оставаться одной из злободневных, при этом меняется не только уровень преступности, но и ее качество в зависимости от изменений, происходящих в обществе особенно в век цифровых технологий. Противодействие преступности может быть эффективным только тогда, когда методы изучения преступности и методы реагирования на преступность будут меняться в соответствии с требованиями времени. В настоящее время в условиях широкого развития и внедрения технологий и коммуникаций проблема борьбы с преступностью не должна рассматриваться в рамках только одной отдельно взятой страны, несмотря на различия национального законодательства, уровня технического развития и материально-технического оснащения, социально-географических особенностей, криминогенных особенностей, образа жизни населения и других причин и условий.

Республика Казахстан активно внедряет современные технологии во все сферы жизнедеятельности общества. Цифровизация названа одним из основных приоритетных направлений развития страны.

На сегодня 77 % населения Казахстана являются интернет-пользователями. Через портал «электронного правительства» предоставляется 761 услуга и сервис. Прогнозируется, что программа «Цифровой Казахстан» позволит достичь темпов роста ВВП страны на уровне 4,5–5 % в год на горизонте с 2025 г. В своем Послании Президент РК назвал цифровизацию стержнем Третьей модерниза-

ции. Нурсултан Назарбаев поручил увеличить производительность труда посредством внедрения новаций для развития массового производства, а также создавать и поддерживать научно-исследовательские институты, которые будут создаваться при предприятиях, а также в ведущих учебных заведениях страны[1]. В то же время новые технологии и их использование во всех их проявлениях всегда были в центре основных дискуссий в сфере борьбы с преступностью, начиная с внедрения самых ранних технологических инноваций.

Поэтому Президент страны особо обозначил актуальность борьбы на современном этапе с киберпреступностью, поручил Правительству и Комитету национальной безопасности разработать концепцию «Киберщит Казахстана», целью которой является обеспечение информационной безопасности общества и государства в сфере информатизации и связи, а также защиты неприкосновенности частной жизни граждан при использовании ими информационно-коммуникационной инфраструктуры[2].

Последние изменения в технологиях были настолько существенными и глубокими, что вызывают особое внимание, поскольку достижения в области информационных технологий, а также в других научных и технических областях произвели глобальную трансформацию во всех сферах жизнедеятельности человека.

В том числе это явилось причиной изменения преступных проявлений. Расширение методов и средств, используемых в преступных целях, так называемых кибер-угроз, актуализировались в двух различных проявлениях:

а) в Интернет мигрировали традиционные виды преступной деятельности, такие как мошенничество, детская порнография, экономические преступления и др.;

б) Интернет способствует таким видам деятельности, как террористические акты, интеллектуальные угрозы, вторжение в различные (общедоступные, частные, коммерческие и др.) сети для нарушения порядка их функционирования. Уязвимость государственных, коммерческих, частных структур от подобного рода преступной деятельности объясняется тем, что критически важные объекты инфраструктуры становятся все более зависимыми от взаимосвязанных компьютерных сетей и Всемирной паутины.

Увеличение количества уголовных правонарушений с использованием информационно-коммуникационных технологий спо-

---

[1] Нурсултан Назарбаев: Цифровизация – это часть индустриальной революции // URL: http://www.inform.kz/ru/nursultan-nazarbaev-cifrovizaciya-eto-chast-industrial-noy-revolyucii.

[2] Государственная программа «Цифровой Казахстан» // www.primeminister.kz.

собствовало выделению в Особенной части Уголовного кодекса Республики Казахстан 2014 г.[1] отдельной главы «Уголовные правонарушения в сфере информатизации и связи». Общественная опасность предусмотренных в данной главе девяти составов уголовных правонарушений заключается в том, что они посягают на охраняемые законом права и интересы граждан и различных организаций, государства и общества в сфере информатизации и связи, нарушают конфиденциальность, доступность, целостность и сохранность информационных систем и ресурсов. Отличительными особенностями уголовных правонарушений данной категории являются их высокая латентность, сложность формирования доказательственной базы, зачастую их транснациональный характер, значительность наносимого материального ущерба, специфичность личности правонарушителя.

Зарубежные ученые, исследовав возможности технологий, используемых на современном этапе в преступных целях и используемых в отношении правонарушителей, предлагают деление инновации в технологиях на две большие категории: «жесткие» технологии и «мягкие» технологии, приводят типы подобных инноваций, которые могут быть использованы в преступных целях, виды неправомерного использования технологий, а также виды, которые могут быть использованы в области предупреждения преступности, деятельности полиции, судов, системе общественного контроля и исправления осужденных, как на институциональном, так и на индивидуальном уровнях[2].

Инновации в «жестких» технологиях включают в себя новые материалы, устройства и оборудование, которые могут быть использованы в совершении любого преступления или его предупреждения и пресечения. Инновации в «мягких» технологиях включают в себя новые программы, программное обеспечение, системы классификации, методы анализа преступлений, совместное использование данных, системы методов интеграции.

В связи с возрастающим значением и ролью цифровых технологий в повседневной жизни, соответственно возникают вопросы: каковы долгосрочные последствия широкого внедрения технологий? Будет ли пропорционально возрастать уязвимость различных структур от преступных посягательств в результате компьютеризации и замены труда человека аппаратными комплексами и програм-

[1] Уголовный кодекс Республики Казахстан. Алматы: Норма-К, 2014. 240 с.

[2] *J.M. Byrne u D.J. Rebovich* The New Technology of Crime, Law and Social Control . 2007.

мами или, наоборот, это будет минимизировать возможности для совершения преступлений отдельными членами общества?

По всей видимости, исходя из предложенной в конце двадцатого века классификации так называемых кибер-преступлений (преступления на работе; преступления как работа; преступления после работы), можно констатировать: однозначный ответ на этот вопрос дать невозможно.

Многие сходятся во мнении, что, пытаясь исключить человеческий фактор из ряда операций в целях оптимизации и повышения эффективности процессов, а в том числе и для исключения возможности преступных посягательств, общество сталкивается с угрозой совершения незаконных деяний в более опасных и масштабных формах.

Технические инновации, используемые как средство для достижения цели, представляются сторонниками различных новых технологий актуальными при условии, что они ведут к повышению производительности, оптимальному решению ряда вопросов социального характера. Однако необходимо учитывать как преднамеренные, так и непреднамеренные последствия продолжающейся борьбы за технологические решения социальных проблем. Опыт отдельных государств демонстрирует немало негативных, а порой и преступных вмешательств в функционирование цифровых аппаратов и комплексов государственного и частного значения. В связи с этим актуальным представляется не только вопрос обеспечения безопасности на уровне использования технологий и его правового регулирования, но и вопрос разработки механизмов укрепления моральной ответственности как на институциональном, так и на индивидуальном уровнях.

Предлагаемые обзоры о возможностях использования современных технологий как в преступных целях, так и в борьбе с преступными посягательствами, к сожалению, устаревают очень быстро, поэтому наибольший акцент, на наш взгляд, следует делать на предупреждении негативных последствий внедрения технологий. Полагаем, одним из перспективных направлений исследований в области внедрения информационных технологий на современном этапе должно стать изучение их использования и неправомерного их использования с социологической точки зрения в превентивных целях.

В условиях, когда преступный мир использует современные научные достижения в сфере информационно-коммуникационных технологий, правоохранительным органам страны необходимо постоянное развитие и максимальное внедрение информационных

систем с целью обеспечения всей правоохранительной системы достоверной и полной информацией.

В данном направлении МВД Республики Казахстан имеет ряд положительных показателей, ведутся работы по созданию новых и доработке существующих информационных систем. Например, Интегрированный банк данных (ИБД) – это ведомственная информационная система централизованного хранения и коллективного использования данных, содержащая информационные массивы, формируемые различными службами и подразделениями органов внутренних дел и других правоохранительных органов, ведомств, взаимосвязанных между собой в едином банке данных.

С целью расширения возможностей ИБД были внесены в базу адреса временной регистрации граждан, информация о составе семьи, сведения о номере свидетельства о смерти, дате выдачи и органе, выдавшем свидетельство, изменен формат загрузки данных о проданных железнодорожных и авиабилетах, добавлен учет «Осужденные» и разработан сервис взаимодействия, планируется наладить получение сведений о наложенных обременениях на автотранспортные средства, а также сведений о приостановлении права вождения.

Координирующим органом по вопросам формирования, совершенствования и интеграции информационно-аналитической системы сегмента МВД, а также определения способов сбора данных, периодичности их предоставления, выработки пороговых значений критериев, необходимых для оценки ситуации, является Информационно-аналитический центр МВД Республики Казахстан.

В рамках продолжения работы по совершенствованию информационного обеспечения ОВД активно развивается взаимодействие с информационными системами других правоохранительных и специальных органов.

Принятие в Республике Казахстан закона «О дактилоскопической и геномной регистрации» позволит создать автоматизированную информационную систему «Биометрическая идентификация личности», в которой будут предусмотрены:

– возможности сбора дактилоскопической информации о гражданах РК, иностранцах и лицах без гражданства, прибывающих в Республику;

– создание базы данных геномной информации, которая будет содержать биологический материал осужденных за совершение тяжких или особо тяжких преступлений, неустановленных лиц, а также биологических родственников без вести пропавших граждан;

– включение биометрических данных о папиллярных узорах рук в документы, удостоверяющие личность гражданина РК, и визы РК.

Собранная информация будет значительно способствовать:

– оперативному подтверждению и (или) установлению личности граждан РК, иностранцев и лиц без гражданства, в том числе по неопознанным трупам;

– выявлению поддельных документов, удостоверяющих личность;

– выявлению лиц, совершивших преступления на территории РК;

– установление родственных отношений разыскиваемых или устанавливаемых лиц. Данная система позволит использовать соответствующую информацию в интересах граждан Республики Казахстан, иностранцев и лиц без гражданства, находящихся в социально опасном состоянии либо являющихся потенциальными жертвами преступлений, аварий и техногенных катастроф, совершенствовать биометрические паспортно-визовые документы.

Также следует отметить международное сотрудничество в сфере информационного взаимодействия. Так, в соответствии с Соглашениями «О взаимоотношениях министерств внутренних дел в сфере обмена информацией» (1992 г., г. Чолпон-Ата) и «Об обмене информацией в сфере борьбы с преступностью» (г. Астана, 22 мая 2009 г.), в рамках Межгосударственного информационного банка, держателем которого является ГИАЦ МВД России, осуществляется взаимообмен информацией.

Одной из важных перспектив развития межгосударственного взаимодействия является организация защищенного канала связи для обмена и использования информации посредством российско-казахстанского сегмента мультисервисной сети «Криминалистика СНГ».

Возможные направления использования цифровых технологий при расследовании преступлений

С. В. Ермаков,
заместитель начальника кафедры,
кандидат юридических наук
(Московский университет МВД России
имени В. Я. Кикотя)

В статье рассматриваются проблемы внедрения и развития цифровых технологий при выявлении, раскрытии и расследовании преступлений.

Расследование преступлений, цифровые технологии, цифровая экономика.

Современное развитие общества обусловливает необходимость внедрения и развития цифровых технологий в различные сферы общественных отношений. Внедрение новых способов организации деятельности, производств с использованием цифровых технологий позволит осуществить переход к новому технологическому укладу.

Цифровые технологии активно используются для совершения различных преступлений, начиная от сбыта наркотиков, хищений денежных средств в кредитных организациях, вплоть до посягательств на жизнь человека, безопасность государства. С другой стороны, цифровые технологии могут оказывать значительную помощь в организации выявления, раскрытия и расследования преступлений.

Стоит обратить внимание на принятие органами власти значительного количества программных документов, направленных на развитие цифровых технологий. Так, распоряжением Правительства РФ от 28.07.2017 № 1632-р утверждена Программа «Цифровая экономика Российской Федерации»[1], разработана Концепция долгосрочного социально-экономического развития РФ на период до 2020 г.; Прогноз социально-экономического развития / научно-технологического развития до 2030 года; Стратегия научно-технологического развития; Стратегия развития отрасли информационных технологий РФ на 2014–2020 годы и на перспективу до 2025 года; Стратегия развития информационного

[1] Собр. законодательства Рос. Федерации. 2017. № 32. Ст. 5138.

общества в Российской Федерации на 2017–2030 годы; Государственная программа «Информационное общество»; План мероприятий («дорожная карта») «Развитие отрасли информационных технологий» и другие[1].

Несмотря на отсутствие прямого указания в данных программных документах на необходимость совершенствования криминалистической деятельности, полагаем, что основные возможности и направления развития цифровых технологий могут быть реализованы при выявлении, раскрытии и расследовании преступлений.

Основными сквозными цифровыми технологиями в рамках программы «Цифровая экономика Российской Федерации» являются: большие данные; нейротехнологии и искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; промышленный интернет; компоненты робототехники и сенсорика; технологии беспроводной связи; технологии виртуальной и дополненной реальностей.

Если рассматривать криминалистическую деятельность как определенную технологию, то можно искать пути ее «цифровизации».

Объективными предпосылками для использования в криминалистической деятельности цифровых технологий являются: высокий уровень компьютерной грамотности следователей, дознавателей, прокуроров, судей, защитников, граждан, вовлеченных в данную сферу; современная техническая оснащенность органов предварительного расследования, прокуратуры, судов для работы в цифровой среде (наличие компьютерной техники, серверов для хранения информации, систем информационной безопасности); наличие электронных цифровых подписей у граждан и должностных лиц; введение электронных паспортов граждан с возможностью использования электронной подписи, биометрическая идентификация личности и прочие условия.

Здесь особо стоит отметить, что биометрическая идентификация личности имеет большой потенциал в сфере борьбы с преступностью, в том числе для деятельности по выявлению, раскрытию и расследованию преступлений. Целесообразно введение обязательной биометрической идентификации граждан РФ в случаях получения, замены паспорта, а также иностранных граждан при въезде на территорию РФ.

---

[1] Официальный интернет-портал правовой информации (www.pravo.gov.ru).

Требуется переход на электронный уровень общения должностных лиц между собой и с гражданами, где это возможно, в рамках уголовного судопроизводства.

Приказом Судебного департамента при Верховном Суде РФ от 11.09.2017 № 168 утвержден Порядок подачи мировым судьям документов в электронном виде, в том числе в форме электронного документа.В судебном следствии проводятся допросы свидетелей с использованием видео-конференц-связи (ст. 278.1.УПК РФ), при соблюдении условий по идентификации их личности. Однако данные возможности вполне возможно распространять и на досудебные стадии.

В части развития криминалистической деятельности можно указать на некоторые потенциальные возможности использования цифровых технологий.

Технология «большие данные» (синонимы – супермассивы данных, BIG DATA) предоставляет новые возможности для осуществления аналитики, выявления скрытых зависимостей и поиск новых вопросов и ответов на основе анализа всего объема разнородных данных. В системе МВД России имеются огромные массивы данных, в том числе не систематизированных. Так, значимая для аналитики информация содержится в материалах уголовных дел, которая в настоящее время не обрабатывается машинным способом. В расследовании преступлений «большие данные» могут использоваться для прогнозирования совершения преступлений в будущем, выдвижения версий, планирования расследования по уголовному делу, розыска скрывшихся от следствия и суда подозреваемых и обвиняемых.

Использование технологий виртуальной реальности уже не ново в криминалистической деятельности отдельных стран, где видеокамеры с возможностью записи 3D панорамных видео применяются при производстве осмотра места происшествия. К примеру, в США уже применяются такие технологии, которые позволяют перенести внешний вид различных мест преступления в виртуальный мир. Судьи при рассмотрении дела могут виртуально погрузиться на место совершенного преступления при помощи очков виртуальной реальности.

Технология искусственного интеллекта может быть применена в автоматизированных онлайн-помощниках следователей (дознавателей) при расследовании уголовных дел. Так, стандартный допрос потерпевшего, свидетеля при совершении типичного преступлении вполне смог бы осуществить онлайн-помощник (технология «Алиса» в Яндексе, «Сири» в Гугле). Причем такой допрос при соответ-

ствующей идентификации личности потенциально может быть осуществлен через удаленный доступ.

В завершение статьи отметим основные выводы.

1) Цифровые технологии в ближайшей перспективе не способны полностью заменить умственную работу следователей, дознавателей, прокуроров и судей.

2) Цифровые технологии должны быть направлены на сокращение затрат времени, производимых на однотипные операции, совершаемые в деятельности следователя (дознавателя), с условием исключения необходимости совершения тех же действий традиционным способом.

3) Финансовые расходы на разработку цифровых технологий должны быть сопоставимы с экономическим эффектом от их внедрения.

4) Внедрение цифровых технологий в криминалистическую деятельность должно сопровождаться проведением пилотных проектов, правовых экспериментов в отдельных регионах.

Основы криминалистической культуры правоприменения и правотворчества

С. Ю. Журавлев,
профессор кафедры,
кандидат юридических наук, доцент
(Нижегородская академия МВД России)

В статье рассматривается феномен криминалистической культуры. Характеризуется сущность криминалистической культуры правоприменения и правотворчества, аргументируется целесообразность применения данного термина.

Криминалистическое знание, криминалистическая культура, правотворчество, правоприменение, криминалистическое мышление, обоснование решений в правотворчестве, обоснование методических и тактических решений в расследовании.

Потенциал криминалистического знания, его огромная роль в правоприменительной деятельности и формировании компетенций будущих юристов позволяет констатировать существование особой криминалистической культуры правоприменения и правотворчества. Важнейшей составляющей данного культурного феномена является специфическое мышление криминалиста, которое лежит в основе процесса познания негативных общественных процессов (явлений), а также обоснования принимаемых решений по установлению обстоятельств расследуемого события. Криминалистическое мышление имеет большие резервы практического применения и дальнейшего совершенствования[1]применительно к процессам правотворчества и правоприменения[2]. По своей сути это

[1] *Журавлев С. Ю.* Методика и организация расследования преступлений как основные факторы эффективной деятельности органов предварительного следствия и дознания // Криминалистические средства обеспечения деятельности по выявлению и расследованию преступлений экономической и коррупционной направленности: сборник статей / [под ред. А. Ф. Лубина]. Казань: изд-во «Бук», 2017. С. 74–78.

[2] *Журавлев С. Ю., Крепышева С. К.* Криминалистическая методика и тактика: контекст современного понимания роли криминалистики в юридической деятельности и юридическом образовании // Современная криминалистика: проблемы, тенденции, перспективы: материалы Международной научно-практической конференции, посвященной 90-летию со дня рождения заслуженного деятеля науки РФ, заслуженного юриста РСФСР, доктора юридических наук, профессора Н. П. Яблокова. Москва, 22 декабря 2015 г. / ред.-сост. М. А. Лушечкина. М.: МАКС Пресс, 2015. С. 49–53.

особая структура мыследеятельности, которая предваряет внешние действия, является условием эффективности принимаемых методических и тактических решений, условием оптимизации процесса правоприменения и правотворчества[1].

С криминалистической точки зрения первично понимание сути происходящих явлений. Логика осмысления и комплексного понимания вредного для общества негативного процесса (явления) требует понять следующее: что и как происходило, кто в этом участвовал, где протекали события, что этому способствовало, что затрудняло совершение определенных действий, насколько распространены конкретные проявления исследуемого негативного процесса (явления) в настоящее время и какова перспектива его развития в будущем. В целом необходимо понять суть той деятельности, последствия которой в социальном плане для нас неприемлемы. Следует осознать результаты этой деятельности как вредные, нарушающие сложившийся порядок, как опасные в целом для общества или отдельных его членов. Криминалистическая направленность данного понимания, ее главная составляющая заключается в обнаружении измененных состояний объектов, которые попали в сферу этой вредной деятельности. Фиксация отличий между исходным состоянием объекта и его конечным состоянием, фиксация информации, содержащейся в измененных состояниях объектов, создает предпосылки для моделирования настоящих и прошлых событий, а также прогнозирования развития ситуации в будущем.

С позиции сущностного понимания познаваемого явления правовая оценка вторична. Она возможна лишь на основе результатов исследования содержания негативного процесса (явления) через призму возникших следов и ни в коем случае не должна опережать процесс сущностного познания реальности. При этом вся сложившаяся система общественных отношений и регулирующих ее правовых норм является нормативным ориентиром для того субъекта, который познает проявления расследуемого негативного процесса (явления). Для субъекта расследования (того, кто следует по следам, распознает их, фиксирует и переосмысливает варианты их практического использования в доказывании) право является ориентиром в понимании того, какие существуют возможные варианты нормативной оценки (квалификации) расследуемого события. При этом

[1] *Журавлев С.Ю.* Комплексная характеристика методических и тактических средств расследования преступлений в сфере экономики // Юридическая наука и практика: Вестник Нижегородской академии МВД России. Н. Новгород, 2016. № 2 (34). С. 141–155.

наиболее негативной тенденцией в этом взаимосвязанном процессе «познания-оценки» является опережающая правовая (уголовная, административная и т. д.) квалификация расследуемого события.

Применительно к процессу расследования можно говорить о трех главных этапах квалификационного мышления: а) предположение квалификационных перспектив в процессе оперативного документирования; б) предварительные квалификационные суждения в стадии возбуждения уголовного дела и предъявления обвинения; в) итоговые квалификационные выводы в процессе составления обвинительного заключения. Именно поэтому, применительно к деятельности по расследованию преступлений, необходимо говорить о приоритете сопровождающего квалификационного мышления субъекта расследования и ступенчатом характере уголовно-правовой квалификации в практической деятельности по расследованию преступлений. С дидактической точки зрения это важно учитывать в процессе моделирования практических задач для учебного процесса, которые должны формировать не столько итоговое (надзорное) квалификационное мышление, сколько способствовать выработке навыка ступенчатого квалификационного анализа с учетом характера вновь поступающей информации.

Опережающее криминалистическое моделирование преступной деятельности исключительно важно применительно к вопросам правотворчества. Определять в законе правовые ориентиры и рамки оценки следует лишь после детального криминалистического исследования негативного общественного явления. До завершения формирования криминалистической характеристики совершенно преждевременно говорить об уголовно-правовой или административно-правовой характеристике. Конструирование (создание) нормы права – это завершающая стадия работы по подготовке изменений в закон. Вначале должна быть дана криминалистическая характеристика вредного для общества процесса (явления), понята суть криминализируемого явления как деятельности, которую предполагается ограничить или полностью исключить из жизни общества. Реальность же такова, что вначале в законе появляются изменения, затем формируется начальная или достаточно устойчивая правоприменительная практика и лишь после этого проводятся научные исследования по формированию криминалистической характеристики данного преступления. Несоблюдение оптимальной, в криминалистическом смысле, технологии правотворчества, в которой обязательно должен присутствовать этап криминалистического моделирования криминального процесса, приводит к вульгаризации в нормах уголовно-

го права понимания структуры и содержания определенного вида преступной деятельности. Как следствие – увеличивается число норм уголовного закона, которые не отражают деятельностный подход к оценке криминальных процессов.

Важный аспект криминалистической культуры связан с пониманием соотношения категорий «методика расследования» и «организация расследования»[1]. О соотношении категорий «организация», «методика» и «тактика» можно сказать, что организация деятельности по расследованию протекает по определенной методике, что организационные мероприятия имеют как методические предпосылки, так и методическое содержание, что применительно к деятельности органа расследования всегда должна разрабатываться и применяться методика управления процессом расследования преступлений, которую не следует смешивать с методикой управления самим органом предварительного расследования, что принятие и реализация конкретных решений в сфере расследования преступлений вытекает из применяемой методики управления процессом расследования и происходит по определенной тактической схеме осмысления подготовки и реализации отдельного тактического действия или их комплекса[2].

Не основанная на научных рекомендациях организация значительно опасней и по своим последствиям страшней, чем отсутствующая методика. Это проявляется во всех элементах организации жизни конкретного подразделения по расследованию преступлений. Никакие методические заделы, никакие научные разработки не заменят отсутствие организационной устремленности на изменения в сторону методического и тактического совершенствования деятельности по расследованию преступлений.

---

[1] *Журавлев С.Ю.* Концепция криминалистического комплекса методических и тактических средств обнаружения и расследования преступлений в сфере экономики // Концепция формирования и использования криминалистического комплекса методических и тактических средств обнаружения и расследования преступлений в сфере экономики: материалы 7-го Межвузовского научно-практического семинара «Раскрытие и расследование преступлений: наука, практика, опыт» (Москва, 12 февраля 2016 г.) / под общ. ред. А.Ф. Волынского, Б.Я. Гаврилова, А.Ф. Лубина. М.: Академия управления МВД России, 2016. С. 73–98.

[2] См. также по данному вопросу: Организация расследования преступлений органами внутренних дел: монография / под ред. Б.Я. Гаврилова. М.: Академия управления МВД России, 2013; *Валов С.В.* Организация расследования преступлений экономической направленности // Организация расследования преступлений органами внутренних дел: курс лекций в 2 ч. / под ред. И.И. Колесникова. М.: Академия управления МВД России, 2011. Ч. 2. С. 34–60; Организация и методика расследования отдельных видов экономических преступлений: уч.-метод. пособие / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: издательство «Спутник +», 2016.

В связи с вышеизложенным вполне обоснованным является важный междисциплинарный вывод о том, что обучение процессу расследования, с криминалистической точки зрения, состоит в привитии навыка принятия методических и тактических решений по сбору, анализу и использованию полученной доказательственной информации[1]. А в части, касающейся вопроса уголовно-правовой квалификации, необходимо говорить, а следовательно и обучать сопровождающему процесс расследования квалификационному мышлению и организационному самоопределению[2]. В его основе должна лежать способность к ступенчатой уголовно-правовой квалификации и пониманию организационной стороны правоприменения. Эту логику профессионального мышления правоприменителя, а также недопустимость опережающих квалификационных суждений и организационных ожиданий следует целенаправленно формировать у обучаемых. Для последовательного формирования криминалистической культуры мышления и принятия решений требуется осознание этапов применения криминалистических дидактических средств, формирующих ключевые компетенции обучаемых[3].

Важнейшей составляющей криминалистической культуры правоприменителя является понимание того факта, что в процессе изучения (познания) конкретных проявлений негативного общественного процесса (явления) применяется не одна, а, как минимум, четыре методики (программы) работы: а) общая (базовая) методика расследования; б) методика работы с первичной информацией; в) методика криминалистического анализа информации, выдвижения, разработки версий и формирования системы доказательств; г) тактико-методический алгоритм обоснования, принятия и реализации решения о проведении отдельного тактического действия или их комплекса.

В основе методического содержания работы по расследованию лежит универсальная логика оперирования условно-вероятностными суждениями по индуктивной и дедуктивной схемам. В процессе индуктивного переосмысления реальности отталкиваются от факта обнаружения первоначальных материальных и идеальных следов. Затем

---

[1] *Журавлев С.Ю.* Понятийные «метаморфозы» предмета доказывания и проблема его конкретизации в методиках расследования экономических преступлений // Российский следователь. ИГ «Юрист». 2008. № 2. С. 2–5.

[2] *Журавлев С.Ю.* Основы формирования криминалистического стиля мышления субъекта расследования преступлений // Современная криминалистика: проблемы, тенденции, имена (к 90-летию профессора Р. С. Белкина): сб. матер. 53-х криминалистических чтений: в 3-х ч. М.: Академия управления МВД России, 2012. Ч. 1. С. 153–159.

[3] *Журавлев С.Ю.* Криминалистические и междисциплинарные инновационные технологии совершенствования учебного процесса // Юридическая наука и практика: Вестник Нижегородской академии МВД России. Н. Новгород, 2015. № 1. С. 198–203.

переходят к моделированию вариантов происшедших событий и тех возможных действий (бездействий), которые привели к возникновению обнаруженных следов. Моделирование и переосмысление особенностей следообразующей криминальной деятельности позволяет предположить существование измененных состояний объектов (следов), которые должны были возникнуть, но пока еще не обнаружены. Их обнаружение и является целью планируемых тактических действий.

В ходе дедуктивного мышления исходят из предположения о том, что некоторое лицо или группа лиц на определенном объекте и в определенных условиях занимается криминальной деятельностью. Затем переходят к моделированию возможных частных направлений деятельности отдельного лица или некоторой группы. В рамках прогнозируемых направлений деятельности моделируются конкретные действия (бездействия) применительно к четырем возможным фазам развития преступной деятельности. После этого переходят на уровень формулировки тех следов, которые объективно возникнут в результате совершения действий (бездействия), которые были смоделированы на предыдущем уровне. Обнаружение следов возможных действий (или бездействия) является целью применения планируемых тактических средств. Сложность указанного процесса заставляет критически взглянуть на периодически повторяющиеся призывы к тому, чтобы криминалисты формулировали простые и доступные для практиков рекомендации по расследованию преступлений. Полагаем, что абсолютно простые криминалистические рекомендации возможны лишь применительно к очень простым криминальным схемам. В них все понятно с первых шагов расследования, применяемое противодействие расследованию минимально[1]. Но более важно понимание того обстоятельства, что относительно простые криминалистические рекомендации возможны лишь применительно к тактическому уровню деятельности по расследованию. Методический уровень работы всегда сложнее, а следовательно текст рекомендаций объективно будет требовать более интеллектуального восприятия. Оно должно быть обеспечено соответствующим криминалистическим образованием и личным опытом самоанализа положительных и отрицательных примеров расследования – по сути дела той самой криминалистической культурой восприятия реальности в процессе правоприменения и правотворчества.

[1] См. напр.: *Лавров В.П.* Противодействие расследованию преступлений и меры по его преодолению: курс лекций. М., 2011; Расследование и противодействие ему в состязательном уголовном судопроизводстве: процессуальные и криминалистические вопросы: сб. науч. трудов. М.: Академия управления МВД России, 2007.

Государственно-частное партнерство при проведении экспертных исследований в сфере высоких технологий

А. П. Земцов
(Ассоциация производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ»)

В статье рассматриваются вопросы проведения экспертных исследований в сфере высоких технологий.

Информационная безопасность, экспертиза, системный анализ, высокие технологии, специальные знания.

Информационная безопасность граждан и организаций, общества и государства подвергается ежедневным непрерывным угрозам. Можно без преувеличения сказать, что в настоящее время перед Российской Федерацией стоят, как никогда прежде, серьезные вызовы национальным интересам в информационной сфере. Данный тезис находит свое подтверждение как в информационных сообщениях СМИ, так и в цифрах аналитических отчетов ведущих компаний в сфере информационной безопасности[1].

Серьезность угроз и важность своевременного и эффективного противодействия им в полной мере осознается и на государственном уровне. Обновленная система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере нашла свое отражение в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[2].

В документе определены стратегические цели и направления обеспечения информационной безопасности, приведены основные угрозы информационной безопасности, а также сформулирова-

---

[1] См.: Отчет о тенденциях высокотехнологичных преступлений компании «Group-IB»: www.group-ib.ru/resources/threat-research/2017-report.html; Отчет Kaspersky Security Bulletin: обзор 2017 года компании «Лаборатория Касперского»: URL: https://securelist.ru/ksb-review-of-the-year-2017/88142.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // URL: http://www.consultant.ru/document/cons_doc_LAW_208191 (дата обращения: 25.04.2018).

ны основные положения политики государства по их выявлению, упреждению и предотвращению.

В обобщенном виде угрозы информационной безопасности представляют собой злонамеренные действия третьих лиц (в широком смысле) в отношении Российской Федерации, бизнеса и граждан, осуществляемые посредством различного рода деструктивного информационно-технического воздействия на инфраструктуру, в том числе критическую инфраструктуру, и (или) информационно-психологического воздействия, то есть пропаганды, – на самих граждан.

Нам представляется, что эти категории угроз обобщенно можно также обозначить как инциденты и преступления, совершаемые с использованием высоких технологий. А как следует из самой природы права и правоприменения – преступления должны влечь за собой обязательность их выявления и расследования.

В настоящее время не вызывает существенных возражений утверждение о том, что эффективное расследование преступлений, совершаемых с использованием высоких технологий, невозможно без применения специальных знаний в форме привлечения в процессуальном порядке специалистов, а также в форме назначения и проведения экспертиз – в основном компьютерно-технических.

И вот именно тут, по нашему мнению, скрыты определенные риски, о которых изложено ниже.

1. На момент подготовки этого материала в Российской Федерации более тридцати высших учебных заведений в той или иной форме осуществляют подготовку специалистов по направлениям, связанным с производством компьютерно-технических экспертиз. Тем не менее, все еще остаются открытыми вопросы о едином содержании преподавания в рамках этой специальности, едином наполнении учебных программ, качестве формируемых у обучаемых практических навыков, выработке единых требований к итоговой аттестации.

Без решения указанных вопросов нет оснований утверждать, что экспертизы, выполненные выпускниками разных вузов, выполнены с сопоставимым уровнем качества, достоверности и глубины погружения в предмет.

2. Не менее важным для поддержания качества производства экспертиз является аспект применения единых стандартов к самому такому процессу. В настоящий момент в Российской Федерации отсутствует какой-либо формальный общепринятый, как минимум на уровне профессионального сообщества, стандарт или набор методик проведения компьютерно-технических экспертиз, а также иных

форм реализации специальных знаний в этой области. Зачастую конкретный эксперт руководствуется исключительно своим собственным профессиональным опытом, но не каким-либо стандартом. Кроме того, до сих пор не решен вопрос о релевантности примененного экспертом какого-либо инструментария экспертным задачам и корректность такого применения с точки зрения регламентов и рекомендаций разработчиков экспертного инструментария.

Совокупность этих факторов приводит к тому, что при возникновении в суде двух противоположных точек зрения, каждая из которых подтверждена заключением эксперта компьютерно-технической экспертизы, суду для разрешения противоречия приходится прибегать к формальной оценке компетенции самих экспертов – путем изучения их профильного образования и профессионального опыта, что не всегда может считаться достоверным критерием оценки качества выполненных исследований.

3. Немаловажным является также и тот факт, что, применяя специальные знания, специалист или эксперт использует определенный инструментарий – специализированное оборудование и программное обеспечение, программно-аппаратные комплексы. Некоторые подобные свойства, которые могут быть известны эксперту, недостатки и ограничения также являются определенным источником риска.

Ниже, в таблице 1, приведен перечень ведущих производителей оборудования и программных продуктов, которые в настоящее время используются при производстве компьютерно-технических экспертиз по всем категориям дел, в том числе – по особо резонансным.

Таблица 1.

Наименование производителя	**Страна происхождения**	**Проприетарный (закрытый) код**	**Сертифицировано в РФ**
AccessData (accessdata.com)	США	да	нет
Paraben (paraben.com)	США	да	нет
Guidance Software (www.guidancesoftware.com)	Канада	да	нет
Cellebrite (cellebrite.com)	Израиль, Япония	да	нет
X-Ways (www.x-ways.net)	Германия	да	нет
Epos (www.epos.ua)	Украина	да	нет

Приведенные в таблице данные позволяют утверждать, что подавляющее большинство экспертных инструментов, применяемых для экспертного обеспечения расследования преступлений, совершаемых с использованием высоких технологий, не проходили какую-либо валидацию в Российской Федерации. Автору также не удалось обнаружить в открытых источниках информацию о том, проводилось ли тестирование этих программных продуктов на отсутствие в них недекларированных возможностей.

Также отметим, что подобное специализированное оборудование и программы создаются без учета требований методического и процессуального характера, вытекающих из особенностей российского судопроизводства, и не учитывают особенности типовых и частных экспертных задач компьютерно-технической экспертизы в рамках правоприменительной практики Российской Федерации.

Заметим, что несмотря на требование ведения судопроизводства в России на русском языке, интерфейсы перечисленных выше программ и формируемые ими отчеты, как правило, англоязычны, не русифицированы. В результате эксперт, выполняющий компьютерно-техническую экспертизу, вынужден интерпретировать результаты работы программы, основываясь на имеющемся уровне знания английского языка.

Разрешение перечисленных противоречий и минимизация указанных выше рисков возможно на основе Доктрины информационной безопасности Российской Федерации, в ст. 33 которой участниками системы обеспечения информационной безопасности, помимо прочих, названы организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности. В связи с этим считаем возможным сделать вывод о том, что компании-производители специализированного программного обеспечения и оборудования, используемого для экспертного обеспечения расследования преступлений в сфере высоких технологий, также являются полноправными участниками единой системы обеспечения информационной безопасности Российской Федерации.

Такой вывод является предпосылкой для решения стратегической задачи консолидации отрасли в целях эффективного участия в системе обеспечения информационной безопасности Российской Федерации.

Законодательством Российской Федерации[1] предусмотрен такой инструмент объединения усилий компаний (то есть юриди-

[1] О некоммерческих организациях: Федеральный закон от 12 января 1996 г. № 7-ФЗ // URL: http://www.consultant.ru/document/cons_doc_LAW_8824.

ческих лиц) в целях представления их общих, в том числе профессиональных, интересов и для достижения общественно полезных целей, как создание ассоциаций, являющихся некоммерческими организациями, основанными на членстве.

Основываясь на данном положении законодательства, в качестве организационного инструмента консолидации в целях разрешения описанных выше задач, была создана Ассоциация производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ».

Ассоциация первоначально учреждена усилиями нескольких российских компаний-участников профессионального рынка производства программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий, в том числе для целей правоприменения, а также оказывающих соответствующие услуги в этой области.

Предметом деятельности Ассоциации «ЭКСПИТ» является:

– взаимодействие с государственными органами в целях представления и продвижения интересов отрасли, в том числе участие в разработке целевых государственных программ, в пределах компетенции;

– популяризация отечественного специализированного программного обеспечения и аппаратных решений, повышение инвестиционной привлекательности этого рынка и его конкурентоспособности на мировой арене;

– поддержание высокого профессионального уровня российских специалистов в сфере экспертных исследований в сфере высоких технологий, включая компьютерную криминалистику и иные, в том числе путем организации образовательных, научных и выставочных программ, конференций, форумов, симпозиумов и иных публичных научно-популярных мероприятий;

– содействие членам Ассоциации в проведении экспертизы, сертификации, стандартизации их решений.

При Ассоциации создан и функционирует Консультативный совет, куда вошли представители экспертных организаций и подразделений федеральных органов исполнительной власти и государственных органов – ЭКЦ МВД России, РФЦСЭ при Минюсте России, Минкомсвязи России, Следственного комитета России. Используя этот инструмент, Ассоциация «ЭКСПИТ» выстраивает не только внутриотраслевой диалог в среде коммерческих компаний, но и активно привлекает к нему государственные судебно-экспертные учреждения, научно-исследовательские

организации, учебные заведения высшего профессионального образования.

Можно сделать вывод о том, что описанная выше деятельность Ассоциации «ЭКСПИТ», по сути, является способом выстраивания партнерских отношений между государством и негосударственными организациям по вопросам, входящим в сферу интересов каждого из участников этого процесса. Таким образом, на наш взгляд, можно условно обозначить эту деятельность как попытку создания некой новой формы государственно-частного партнерства, не отраженной в действующем законодательстве[1], а именно – государственно-частное партнерство в сфере обеспечения информационной безопасности Российской Федерации, в том числе при проведении исследований в рамках экспертного сопровождения (обеспечения) расследования преступлений в сфере высоких технологий.

Одним из практических результатов деятельности Ассоциации «ЭКСПИТ» в рамках указанного условного государственно-частного партнерства является создание, при поддержке экспертного сообщества, методических рекомендаций по исследованию современных мобильных устройств в уголовном судопроизводстве. Данный документ является первой попыткой на уровне отрасли и экспертного сообщества прийти к единым стандартам работы, в том числе в целях повышения качества экспертного сопровождения (обеспечения) расследования преступлений в сфере высоких технологий.

Представляется обоснованным провести более глубокий и системный анализ открывающихся в рамках работы Ассоциации «ЭКСПИТ» возможностей по повышению уровня обеспечения информационной безопасности Российской Федерации и, в случае выявления существенной пользы от использования такой формы взаимодействия, – внести соответствующие предложения об изменении законодательства в части регулирования сферы применения государственно-частного партнерства, дополнив ее деятельностью по обеспечению информационной безопасности и экспертного сопровождения (обеспечения) расследования преступлений в сфере высоких технологий.

---

[1] О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 13 июля 2015 г. № 224-ФЗ // URL: http://www.consultant.ru/document/cons_doc_LAW_182660 (дата обращения: 25.04.2018).

Некоторые аспекты применения специальной криминалистической техники в раскрытии преступлений

А. Н. Калюжный,
кандидат юридических наук, доцент

В статье исследуется специфика применения специальной криминалистической техники для извлечения криминалистически значимой информации из средств сотовой связи, анализируются технические средства, предназначенные для обнаружения средств сотовой связи, обосновываются основы процессуального закрепления полученных результатов.

Специальные знания, технические средства, расследование, преступления, сотовая связь.

Развитие технологий и внедрение достижений научно-технического прогресса в механизм совершения современных преступлений детерминирует необходимость повышения качества научно-методического и технико-криминалистического обеспечения расследования преступлений, одним из приоритетных направлений которого является использование специальных знаний и специальной криминалистической техники.

Проблемы применения специальной криминалистической техники в ходе расследования преступлений породили множество полемических вопросов и привлекли внимание целого ряда ученых-криминалистов, развернувших дискуссию в данной сфере. Не останавливаясь на исследовании теоретических положений и практических затруднений использования специальных знаний[1], поскольку это выходит за границы предмета анализируемой проблематики, рассмотрим лишь некоторые из них.

В настоящее время одним из технических средств, применяемых преступниками по посягательствам, являются мобильные телефоны сотовой связи, с помощью которых согласуются и координируются преступные действия виновных, предъявляются угрозы

[1] См., например: *Гаврилов Б. Я.* О некоторых правовых проблемах использования специальных знаний в стадии возбуждения уголовного дела // Научные портал МВД России. 2015. № 1 (29) С. 5–10; *Майлис Н. П.* Современные проблемы научных и методологических основ судебной экспертизы // Вестник экономической безопасности. 2016. № 3–2. С. 91–95; и др.

и требования преступников, определяются действия сообщников по подготовке и сокрытию преступной деятельности и т. п. Современные возможности средств мобильной связи позволяют не только осуществлять звонки и обмениваться сообщениями посредством сотовой связи, но и использовать для общения и передачи информации интернет-технологии различных программных средств (Telegram, WhatsApp, Skype и др.) и социальных сетей (ВКонтакте, Одноклассники, Facebook и др.).

Несмотря на непосредственность воздействия мобильных телефонов сотовой связи на механизм совершения преступлений, механизм их следообразования имеет свою специфику, поскольку образованные ими следы не отображаются во внешней материальной обстановке, нося информационный характер. Использование специальных знаний в ходе расследования преступлений позволяет не только выявить и зафиксировать оставленные с помощью мобильных средств сотовой связи следы преступной деятельности, но и установить местонахождение преступника или похищенной им жертвы, определить маршрут их перемещения, восстановить текстовую и мультимедийную информацию, переданную с помощью мобильного устройства и выяснить принадлежность переданных данных конкретному лицу.

Современное обеспечение субъектов расследования специальной криминалистической техникой позволяет извлекать полную информацию, включая удаленную, из содержимого и памяти мобильных устройств, электронных накопителей информации, SIM-карт, записывающих устройств и т. п. на любом этапе расследования, в том числе и предварительном. Наибольшую распространенность у субъектов расследования получили такие виды специальной криминалистической техники, как: универсальное устройство извлечения судебной информации (UFED – UniversalForen sicExtractionDevice), мобильный криминалист, XRY, MOBILedit, Тарантула и др.).

Не останавливаясь на обосновании назначения и анализе особенностей каждого из видов специальной криминалистической техникой, обратим внимание на возможности серии универсальных устройств извлечения судебной информации (UFED), эффективность которого подтверждается судебной и следственной практикой расследования преступлений. Программное обеспечение UFED TouchUltimate позволяет получить информацию о телефоне (IMEI/ESN); SIM-карте (ICCID и IMSI); датах, времени, длительности вызовов, в том числе удаленных; направленных SMS, MMS и голосовых сообщениях и переданных по

ним фото-медиа-файлах, в том числе удаленных; записях телефонной книги и др[1].

Универсальное устройство извлечения судебной информации позволяет извлекать и восстанавливать данные из программного обеспечения сети Интернет, установленного на изъятиях мобильных устройств: сообщения чатов и электронной почты; изображения; видео- и аудиофайлы; определять местоположение преступников или потерпевших в определенное время и дату; устанавливать маршруты перемещения; вскрывать пароли журналов вызовов, текстовых сообщений, контактов в электронной почте. Значительным преимуществом анализируемого программного комплекса является возможность восстановления данных в получивших распространение в России и за рубежом мессенджерах – системах мгновенного обмена сообщениями (Telegram, WhatsApp, Viber и др.), а также переписки в различных социальных сетях (ВКонтакте, Одноклассники, Twitter, Facebook и др.)[2].

Использование возможностей специальной криминалистической техники на предварительном и первоначальном этапах расследования позволяет установить местонахождение и маршруты передвижения участников судопроизводства, выявить причастность отдельных лиц к преступным посягательствам, а на последующем этапе расследования – напрямую изобличать виновных в исследуемых посягательствах и способствовать всестороннему установлению обстоятельств уголовного дела.

Процессуальное оформление результатов использования специальной криминалистической техники возможно путем составления протокола осмотра предметов, с привлечением специалиста или же назначения компьютерно-технической (информационно-аналитической) экспертизы, что, на наш взгляд, является более предпочтительным, поскольку извлечение и анализ криминалистической информации из мобильного устройства может занять значительный период времени. Законность производства осмотра предметов, содержащих информацию, ограничивающую конституционные права граждан, без получения судебного решения подтвердил в своем

[1] *Рогова И. А., Бурцева Е. В.* Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств // Евразийский союз ученых. 2015. № 7 (16). С. 97–100.

[2] *Скобелин С. Ю.* Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 31–33.

определении Конституционный Суд Российской Федерации[1], а процессуальный порядок получения судебных решений на производство соответствующих следственных действий уточнил в своем постановлении Пленум Верховного Суда Российской Федерации[2].

На предварительном этапе расследования использование специальной криминалистической техники возможно в ходе производства таких оперативно-розыскных мероприятий, как контроль почтовых отправлений, телефонных и иных сообщений или снятия информации с технических каналов связи.

Эффективность использования специальной криминалистической техники подтверждается материалами судебной и следственной практики. Например, Никифоров Д. И., Баранов Е. Н., Зайцев К. М., Нечаев Д. С. и Масленников А. А. из корыстных побуждений, направленных на формирование намерения у потерпевшего Лебедева А. А. к продаже его квартиры, по предварительному сговору между собой путем причинения телесных повреждений совершили похищение Лебедева А. А., затолкав его в автомобиль и перевезя к местам содержания (гараж, затем квартира).

В качестве одного из доказательств общения фигурантов друг с другом нахождения их в определенное время и в конкретных местах содержания потерпевшего явился протокол осмотра предметов (документов), которым проведен анализ осмотренных телефонных соединений подсудимых и указано: «дата и время выхода телефона с IMEI №... SIM-картой №... абонентским номером... зарегистрированным на гражданина.... выходил в эфир в районе ближайшей базовой станции по адресу... имели место соединения с номерами.... принадлежащими... и т. д.»[3], тем самым изобличив подозреваемых в совершенных преступлениях.

---

[1] Определение Конституционного Суда Российской Федерации от 8 апреля 2010 г. № 430-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Николая Алексеевича на нарушение его конституционных прав частью первой статьи 176 и частью первой статьи 285 Уголовно-процессуального кодекса Российской Федерации» // СПС «Гарант».

[2] Постановление Пленума Верховного Суда Российской Федерации от 1 июня 2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» // Бюллетень Верховного Суда РФ. 2017. № 7. Июль.

[3] Архив Воскресенского городского суда Московской области // Уголовное дело № 22-823/2015 по обвинению Никифорова Д. И., Баранова Е. Н., Зайцева К. М., Нечаева Д. С. и Масленникова А. А. в совершении преступлений, предусмотренных п.п. «а», «в», «г», «з» ч. 2 ст. 126, п. «б» ч. 3 ст. 163 УК РФ.

Подводя итоги изложенному, отметим, что эффективность расследования преступных посягательств требует обширного использования специальных знаний и современных возможностей специализированной криминалистической техники. Не вызывает сомнений, что использование современных криминалистических технологий, новых, нетрадиционных методик проведения экспертных исследований, специальной криминалистической техники, возможностей информационно-телекоммуникационных систем и аппаратно-программных комплексов значительно расширяют потенциал субъектов расследования по раскрытию и расследованию преступных посягательств.

Исследования компьютерных информационных процессов в структуре науки криминалистики

В. Н. Карагодин,
доктор юридических наук, профессор
(Московская академия Следственного комитета Российской Федерации)

В статье рассматриваются предложения о расширении объекта и предмета криминалистики, высказываются критические замечания по поводу разработки криминалистического учения о компьютерной информации (электронной криминалистике).

Компьютерные средства, технологии, информация; криминалистическое учение о компьютерной информации.

В последнее время активизировались выступления в печати сторонников расширения объекта и предмета криминалистики, изменения ее структуры в связи с появлением и якобы бурным ростом компьютерных преступлений. Несмотря на отрицательную динамику преступлений названного вида, они не являются преобладающими в общем количестве совершаемых в нашей стране уголовно-наказуемых деяний. Кроме того, распространенность тех или иных преступлений и даже неудовлетворительный уровень их раскрываемости еще не свидетельствует о необходимости изменения парадигм криминалистики.

В теории криминалистики возможности использования кибернетических методов исследовались задолго до появления не только компьютерных преступлений, но и компьютерных технологий. Среди них могут быть названы изыскания авторов, вплотную подошедших к реализации названных методов в проведении почерковедческих[1] и дактилоскопических[2] экспертиз. Фактически одновременно проводились изыскания и внедрялись в практику органов предва-

[1] *Козинец Б. Н., Ланцман Р. М., Якубович В. А.* Об одном кибернетическом методе исследования в криминалистической экспертизе почерка // Кибернетика и судебная экспертиза. Вильнюс, 1966. Вып. 2. С. 55–84; *Асатурян В. И., Эджубов Л. Г.* О некоторых принципах построения алгоритмов анализа почерка идентификационного типа // Правовая кибернетика. М., 1973. С. 176–186.

[2] *Эджубов Л. Г.* О критерии дактилоскопического тождества / Л. Г. Эджубов, Б. С. Брудовский // Правовая кибернетика. М., 1973. С. 219–237.

рительного расследования рекомендации об использовании ЭВМ для поиска преступников по способу посягательства[1].

Кроме признания за первыми исследователями приоритета анализируемой темы нельзя не обратить внимание, что они использовали достижения новейших для того времени технологий для выполнения отдельных операций, так или иначе связанных с уголовным судопроизводством. При этом и речи не шло о приспособлении, адаптации деятельности по применению норм уголовного, материального и процессуального права к специфическим условиям использования компьютерных технологий. Думается, что это было обусловлено не только недостаточно высоким уровнем компьютеризации в нашей стране. Подход ученых к решению данной проблемы основывался на принципе объективной оценки отсутствия потребностей в изменении правил и процедур регулирований. Если речь идет о нормативных предписаниях, то они должны не приспосабливаться к объективной реальности, а обеспечивать сохранение благоприятных, полностью устранять существование или блокировать влияние неблагоприятных для регулирования названных правоотношений условий.

В криминалистике достаточно давно предпринимались попытки создания так называемой «Криминалистической информатики»[2].

В последнее же время появились публикации, содержащие предложения о разработке криминалистического учения о компьютерной информации или «электронной криминалистики»[3].

Удивительно стремление наших авторов обозначить как криминалистические учения теории самых разных теоретических построений, в основе которых лежат слабо аргументированные, а то и вовсе никак не аргументированные утверждения об особенностях исследуемого объекта. Специфика объекта якобы требует разработки частной криминалистической теории (учения). Далее подходит подгонка предлагаемого построения под признаки криминалистического учения.

Подобными недостатками отличаются построения, которые обозначаются как криминалистическое учение о компьютерной информации.

---

[1] *Горшков А. Ф., Девиков Е. И., Зуйков Г. Г.* Вопросы автоматизации поиска преступников по способу совершения преступления и признакам внешности // Вопросы борьбы с преступностью. М.: Юрид. лит., 1970. № 12. С. 102–113; *Зуйков Г. Г.* Применение математической логики и ЭВМ для решения криминалистических задач на основе «модус операнди» // Правовая кибернетика. М., 1973. С. 143–152.

[2] *Толстолуцкий В. Ю.* Криминалистическая информатика. Ижевск, 2003.

[3] *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис. ... д-ра. юрид. наук / Вехов В. Б. Волгоград, 2008. 45 с.

Предлагаемое содержание анализируемой теории вызывает большие сомнения в том, что ее предмет является частью предмета криминалистики. Как известно, в настоящее время превалирующей в нашей стране является теоретико-доказательственная концепция предмета криминалистики. В соответствии с ней к предмету криминалистики относятся закономерности возникновения, собирания, исследования (проверки и оценки), а также использования доказательственной информации.

Под эти закономерности очень легко подгоняется любая предметная область, в том числе закономерности, касающиеся компьютерной информации. В обосновании специфичности этого явления в структуре предлагаемого учения выделяется еще одно криминалистическое учение компьютерной информации. Сложность предлагаемой структуры названного учения привела автора к путанице. Криминалистическое учение о компьютерной информации он называет подразделом криминалистического исследования[1]. Учение, частная теория представляет собой систему положений, выводов, суждений. Исследование же – это процесс изучения. Это мелкий недостаток, который тем не менее свидетельствует о том, что предлагаемая конструкция далека от совершенства.

Основное возражение вызывают утверждения сторонников анализируемой теории о том, что специфика информации и обстановки, в которой она возникает, хранится, обрабатывается и передается, исключает возможность применения для их обнаружения, исследования и использования криминалистических методов в целом[2].

Нельзя согласиться и с существованием криминалистического понятия компьютерной информации. Эта дефиниция должна отражать признаки общего понятия информации и специфики компьютерной. Последняя связывается, прежде всего, с электронно-цифровой формой хранения, передачи и обработки анализируемого вида информации[3].

---

[1] *Вехов В. Б.* «Электронная криминалистика»: что за этим понятием? // Проблемы современной криминалистики и основные направления ее развития в XXI веке: материалы Международной научно-практической конференции, посвященной 60-летнему юбилею кафедры криминалистики Уральского государственного юридического университета (6 октября 2017 г.). Екатеринбург, 2017. С. 79.

[2] *Ищенко Е. П.* Киберпреступность: криминалистический аспект проблемы // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 185–186.

[3] *Зигура Н. А., Кудрявцева А. В.* Компьютерная информация как вид доказательств в уголовном процессе России. М., 2011. С. 24.

Важным сущностным признаком является электромагнитный метод обработки и ее хранение на специальном носителе[1].

Однако компьютерная информация может быть преобразована в письменные тексты, а также видео-фото изображения запечатлеваемых объектов.

Таким образом, компьютерная информация возникает и существует в электромагнитных полях в закодированной форме и может быть воспроизведена в привычном для восприятия человеком виде. Представляется, что не может быть никакого криминалистического понятия «компьютерная информация». В криминалистике может использоваться понятие этого явления, разработанное соответствующими специалистами. Процессы и закономерности возникновения компьютерной информации становятся частью объекта и предмета криминалистики, когда они связаны а) с совершением; б) с расследованием преступления.

В первом случае релевантная компьютерная информация возникает в результате использования в процессе подготовки, совершения и сокрытия преступлений средств компьютерной техники и современных электронных технологий.

Во втором – компьютерные устройства и технологии используются для обнаружения, исследования и фиксации любых других фактических данных. Чаще всего они используются в качестве средств фиксации. В настоящее время практически все протоколы следственных действий, иные процессуальные документы набираются и печатаются с помощью средств компьютерной техники.

В связи с этим возникает вопрос – все ли процессы и закономерности компьютерной информации, связанные с совершением и расследованием преступлений, должны изучаться криминалистикой? Ответ на этот вопрос должен быть отрицательным. Объектом и предметом криминалистики могут быть только те явления, исследование которых не требует специальных познаний из других отраслей науки. Поэтому компьютерно-техническая экспертиза и специальные исследования компьютерных средств с целью обнаружения информации, скрываемой с помощью технических приемов и методов, идентификации автора программного продукта и т. п., не относятся к числу криминалистических. При проведении подобных экспертиз и исследований требуются специальные познания в области компьютерных техники и технологии, а также приемы и методы, выработанные другими науками.

---

[1] *Быков В. М., Черкасов В. Н.* Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы. М., 2015. С. 47–48.

В связи с этим уместно напомнить, что Р. С. Белкин предостерегал от необоснованного поглощения криминалистикой естественных и технических наук[1]. Это предостережение актуально, в частности, для инициаторов создания как нового раздела криминалистической техники,[2] так и криминалистического учения, охватывающего положения криминалистической техники и тактики. Процессы возникновения электронных следов относятся к компетенции специалистов в области кибернетики, электроники и математики. Все остальные следы, по нашему мнению, в достаточной мере исследуются в рамках уже существующих разделов криминалистической техники.

Это касается и положений следственной тактики. В настоящее время не усматривается потребностей практики в разработке тактических приемов проведения следственных действий с целью обнаружения средств компьютерной техники и компьютерной информации. Организационные особенности производства подобных действий вполне достаточно и ясно излагаются вместе с рекомендациями по исследованию отдельных видов объектов.

Высказанные суждения не означают, что инициативы критикуемых авторов не имеют права на жизнь. Возможно, дальнейшие усилия этих ученых по формированию предлагаемых теоретических построений приведут к положительным результатам. При этом подвижникам новых идей следует помнить, «что попытки превратить криминалистику в меганауку со ссылкой на ее интегративную природу ведут к разрушению ее сущности и предмета...»[3].

---

[1] *Белкин Р. С.* Общая теория советской криминалистики. Саратов, 1986. С. 157.

[2] *Демин К. Е.* К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники // Библиотека криминалиста. Научный журнал. 2013. № 5. С. 176–177.

[3] *Смахтин Е. В.* Криминалистика: кризис или необходимость уточнения содержания предмета? // Российское право. 2017. № 5 (102). С. 27.

Электронные носители информации: некоторые проблемы теории и практики

Л. В. Кокорева,
доцент кафедры,
кандидат юридических наук
(Московский областной филиал МосУ
МВД России)

В статье обращено внимание на некоторые проблемы теории и практики изъятия электронных носителей информации. Автором проанализированы действующее законодательство, мнение ученых, следственная практика по рассматриваемому вопросу. Предлагается внести ряд изменений в законодательство по улучшению правоприменительной практики.

Электронные носители информации, следственные действия, обыск, выемка.

На сегодняшний день проблема изъятия электронного носителя информации, как нового источника доказательств по уголовному делу, при производстве следственных действий является весьма актуальной. Безусловно, применение в преступной деятельности информационных технологий и активное использование сети Интернет привело к внесению соответствующих изменений в уголовно-процессуальное законодательство. В частности, Федеральный закон от 28.07.2012 № 143-ФЗ[1] внес изменения в ст.ст. 81, 82, 166, 182, 183 УПК РФ, дополнив их электронным носителем информации. Отметим, что участие специалиста при изъятии электронных носителей информации в ходе производства таких следственных действий, как обыск и выемка, является обязательным.

Обратим внимание, что внесение рассматриваемым Федеральным законом № 143-ФЗ изменений обусловлено появлением новых информационных технологий и необходимостью соответствия уголовно-процессуальных норм уровню развития общества. Однако содержание вводимых норм нельзя признать совершенными[2]. Результаты анализа практики позволяют утверждать, что отсут-

[1] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 28 июля 2012 г. № 143-ФЗ. URL:http://www.consultant.ru/document/ (дата обращения: 25.10.2015).

[2] *Ларин Е. Г.* Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. 2012. № 2 (29). С. 52–53.

ствие в законе детально прописанного порядка изъятия и исследования электронных носителей информации порождает разную правоприменительную практику, что, бесспорно, усложняет деятельность следователей (дознавателей).

А. Н. Першин, изучая проблемные вопросы применения электронных носителей информации в практической деятельности, в 2014 г. провел опрос следователей и дознавателей органов внутренних дел из 14 субъектов РФ. Данный опрос показал, что исследуемая проблема более чем актуальна. Так, в 53 % случаев респонденты испытывали серьезные затруднения именно при работе с информацией в электронном формате[1].

В свою очередь, поскольку уровень технического развития общества с каждым годом возрастает, наметилась положительная тенденция в работе с электронными носителями информации. Так, по результатам проведенного нами в 2017 г. опроса следователей Московской и Смоленской областей можно утверждать, что большинство следователей испытывают незначительные проблемы при работе с электронными носителями информации (46 % случаев), причем, зачастую, эти проблемы носят организационный характер.

Сам термин «электронный носитель информации» с юридической и технической точек зрения имеет различную трактовку. Возникает вопрос: что же считать электронным носителем информации? В ст. 5 УПК РФ данное понятие отсутствует.

В соответствии с межгосударственными стандартами под электронным носителем информации понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники»[2]. По мнению П. В. Козловского, П. В. Седельникова, «электронный носитель» является достаточно широким понятием, охватывающим не только магнитные накопители серверов, но и flash-накопители, CD, DVD-диски, сотовые телефоны и т. п.[3] Некоторые ученые выразили негативное отношение к появлению данного термина в УПК РФ, посчитав, что это только один вид машинных носителей, который не охватывает магнитные и оптические носители информации.

---

[1] *Першин А. Н.* Электронный носитель информации как новый источник доказательств по уголовному делу // Уголовный процесс. 2015. № 5. С. 50.

[2] ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения (введен в действие приказом Росстандарта от 22.11.2013 № 1628-ст) // СПС «КонсультантПлюс».

[3] *Козловский П. В., Седельников П. В.* Участие специалиста в изъятии электронных носителей // Научный вестник. 2014. № 1. С. 18.

Кроме понятия и значения, достаточно остро на практике обсуждается сама процедура изъятия электронного носителя информации. Привлечение специалиста, обладающего знаниями в области информационных технологий, затруднительно ввиду их небольшого числа в экспертных учреждениях. Решается данная проблема путем привлечения к производству следственных действий специалистов, которые не являются сотрудниками экспертно-криминалистических подразделений. Это могут быть сотрудники научно-исследовательских институтов (специализирующиеся на изучении, хранении, передаче, обработке, защите и воспроизведения информации с использованием компьютеров[1]), технические специалисты коммерческих учреждений, в чьи функции входит установка компьютерных систем, программного обеспечения, ремонт компьютерной техники и т. д., а также преподаватели информатики.

Кроме изъятия электронных носителей информации специалист оказывает помощь в копировании информации. При этом законодатель запрещает осуществлять копирование информации, если это может воспрепятствовать расследованию преступления либо по заявлению специалиста повлечь утрату или изменение информации. Решение об удовлетворении ходатайства о копировании информации должен принимать исключительно следователь (дознаватель), т. к. именно он несет персональную ответственность за расследование уголовного дела, в том числе и за хранение доказательственной информации, полученной при производстве следственных действий.

Как ранее отмечалось, законодатель предусматривает обязательное участие специалиста при изъятии электронных носителей информации при производстве обыска и выемки (ч. 9.1 ст. 182, ч. 3.1 ст. 183 УПК РФ). В свою очередь обратим внимание на то, что данное положение вступает в противоречие с ч. 1 ст. 168 УПК РФ, в которой следователю предоставляется право по своему усмотрению привлекать специалиста к производству следственных действия. При этом заметим, что участие специалиста зачастую не является оправданным. К примеру, при изъятии флеш-накопителя, CD, DVD-диски, сотовых телефонов и т. д. Данные электронные носители информации следователь (дознаватель) может самостоятельно обнаружить, изъять, упаковать при производстве обозначенных следственных действий. В практической деятельности необходи-

[1] Материал из Википедии – свободной энциклопедии. Портал: Компьютерные технологии. URL:https://ru.wikipedia.org/wiki (дата обращения: 23.04.2018).

мость обеспечения участия специалиста усложняют производство следственных действий.

В научной литературе высказывается и иная точка зрения. Так, ряд ученых полагает, что участие специалиста следует признать обязательным, но лишь в определенных ситуациях. Причем в качестве специалиста надлежит привлекать лицо, обладающего «глубокими знаниями в сфере функционирования программного и аппаратного обеспечения обследуемых электронных устройств, а в отдельных случаях он должен разбираться в более сложных специфических вопросах (особенностях эксплуатации сетевого оборудования, процедурах шифрования информации и т. п.), иметь достаточные навыки их практического решения (например, владеть методикой применения криминалистических средств выявления и фиксации доказательств)»[1]. Трудно не согласиться с данным предложением. Полагаем, что привлечение к производству следственных действий специалистов, не сведущих в сфере информационных технологий, лишь усложняет процесс расследования.

В заключение отметим, что в УПК РФ достаточно часто используется понятие «изъятие» в вопросах производства следственных действий, однако определение данному понятию законодателем не дано. Обоснованно возникают вопросы: можно ли считать изъятие самостоятельным действием или оно является составной частью каких-то следственных действий (к примеру, ч. 1 ст. 144 УПК РФ)? И если да, то каких? В данном случае уместны доводы А. Р. Белкина, который предлагает дополнить УПК РФ новой статьей – 164.1. «Изъятие предметов, документов, образцов»[2]. Разделяя мнение ученого, отметим, что вводимая норма должна содержать понятие изъятия, перечень следственных действий, в рамках которых оно допустимо, процессуальный порядок и удостоверительный характер данного действия. Кроме этого, поддерживая мнение А. Л. Осипенко, А. И. Гайдина, считаем целесообразным более четко закрепить в законе перечень электронных носителей информации, к которым применяется особый порядок изъятия[3].

---

[1] *Осипенко А. Л., Гайдин А. И.* Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 160.

[2] *Белкин А. Р.* УПК РФ: конструктивная критика и возможные улучшения. Ч. IX. Следственные действия. М.: МГУПИ, 2014. С. 10.

[3] *Осипенко А. Л., Гайдин А. И.* Указ. соч. С. 158.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами: организация и тактика следственного действия

Д. Л. Кокорин,
начальник кафедры,
кандидат юридических наук, доцент
(Уральский юридический институт
МВД России)

Р. А. Дерюгин,
адъюнкт
(Уральский юридический институт
МВД России)

В статье рассматриваются некоторые организационные и тактические особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами. Авторы указывают на проблемы, связанные с появлением данного следственного действия, обусловленного активным развитием и повсеместным распространением современных технических средств сотовой связи.

Информация, абонент, абонентские устройства, следователь, расследование, тактика.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие было закреплено в Уголовно-процессуальном кодексе Российской Федерации (далее – УПК РФ) 1 июля 2010 г.

Несмотря на начало эпохи развития информационного общества, появление нового процессуального инструмента, направленного на получение информации об абонентах, детализации вызовов, геоположении абонентских устройств связи, вызвало массу неоднозначных споров и дискуссий. Ряд авторов высказываются критично, обосновывая, что получение информации о соединениях между абонентами и (или) абонентскими устройствами нельзя в полной мере относить к следственным действиям[1]. Другие отме-

[1] *Кальницкий В. В.* Вопросы правовой регламентации следственных действий на современном этапе // Законы России: опыт, анализ, практика. 2015. № 2. С. 34; *Безлепкин Б. Т.* Краткое пособие для следователя и дознавателя / Б. Т. Безлепкин. М., 2011. С. 80.

чают исключительно положительные моменты, связанные с нововведениями[1]. Несмотря на то, что получение информации о соединениях между абонентами и (или) абонентскими устройствами активно используется следственными органами при расследовании преступлений более семи лет, в науке остаются нерешенные вопросы, касающиеся организации и тактики данного следственного действия.

Во-первых, это связано с тем, что некоторые ученые относительно рассматриваемого следственного действия предпочитают говорить о «технологии», нежели о «тактике»[2]. Объясняется такая точка зрения следующим образом. Тактика применима там, где необходимо преодолевать противодействие, есть соперничество или несовпадение интересов, а технология – это наиболее целесообразный способ проведения трудовых операций, без оказания противодействия. На первый взгляд, все логично, так как действительно получение информации о соединениях между абонентами и (или) абонентскими устройствами технически сложное следственное действие, которое требует привлечения оператора сотовой связи, объединяет в себе признаки других следственных действий и не предполагает противодействия. Однако если обратиться к этимологии терминов, то технология относится к определенной области, методам и способам производства, а тактика – это совокупность методов и приемов, направленных для достижения цели[3]. Очевидно, что термин технология не вполне уместно употреблять в контексте со следственными действиями.

Во-вторых, в силу комплексного характера следственного действия, предусмотренного ст. 186.1 УПК РФ, не сложилось единой точки зрения по поводу разграничения этапов тактики его проведения. Четких границ, где начинается и заканчивается рабочий этап, нет, в связи с этим мнения ученых разняться.

---

[1] *Трухин С.* Надлежащие доказательства как основание для разрешения судом следственных действий, ограничивающих конституционные права граждан // Уголовное право. 2012. № 6. С. 94–102; *Стельмах В. Ю.* Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В. Ю. Стельмах. Екатеринбург: Уральский юридический институт МВД России, 2014. С. 40.

[2] *Центров Е. Е.* Особенности использования положений следственной тактики в правоприменительной деятельности // Криминалистика в системе правоприменения. Материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М. В. Ломоносова. М., 2008. С. 25 – 26; *Белкин Р. С.* Курс криминалистики: учебное пособие для вузов. 3 изд., дополненное. М., 2001. С. 599.

[3] *Ожегов С. И.* Толковый словарь русского языка / С. И. Ожегов, Н. Ю. Шведова. URL: http://slovarozhegova.ru/word.php?wordid=31378.

В-третьих, очень важным моментом в рамках тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами видится вопрос о принятии решения о производстве следственного действия. Именно на этом этапе анализируются факты и сведения, которые влияют на принятие следователем решения о целесообразности проведения того или иного следственного действия в рамках сложившейся следственной ситуации. Остается только решить, рассматривать ли момент принятия решения в структуре этапов тактики следственного действия, тем самым значительно расширив ее, или отдельно от нее.

В целях разрешения указанных проблем представляется необходимым рассмотреть получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре этапов тактики следственного действия.

Как уже было отмечено, указанное следственное действие – технически сложное и комплексное, а также влечет ограничение конституционных прав гражданина, поэтому немаловажным является момент принятия решения о его производстве. Данное решение следователя должно быть логичным и взвешенным, исходя из сложившейся следственной ситуации. Так как выбор рассматриваемого следственного действия связан с вмешательством в сферу конституционных прав граждан, следователь обязан определиться, насколько обоснованно такое решение и соразмерно целям расследования. В связи с этим считаем, что принятие решения о производстве любого следственного действия, как тактический аспект, необходимо рассматривать в рамках тактики расследования в целом, не включая его в структуру этапов тактики конкретного следственного действия. Именно после принятия решения о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами реализуются дальнейшие мероприятия, соответствующие подготовительному, основному и заключительному этапам следственного действия.

Подготовительный этап получения информации о соединениях между абонентами и (или) абонентскими устройствами условно можно разделить на две стадии. Действия первой стадии проводятся до вынесения постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами. На этом этапе изучаются материалы уголовного дела, устанавливаются данные об абоненте или абонентском номере, при этом особенно важно как можно больше знать о лице, чьи соединения будут проверяться, а также направ-

ляются запросы в компании операторов сотовой связи на предмет отношения абонентского номера или абонентского устройства к конкретной компании. Вторая стадия подготовительного этапа выполняется, когда становится известно о факте регистрации абонента у того или иного оператора связи. В этом случае в постановлении указываются те моменты, которые необходимы для расследования уголовного дела. Например, можно запросить: входящие/исходящие вызовы (дата, время, продолжительность соединения); входящие/исходящие SMS (дата, время получения или отправки, номер получателя); данные SIM-карты (сведения об абоненте); геолокацию абонентского устройства; идентификационный код IMEI; координаты места осуществления соединений, отправки сообщений, использования интернет-трафика.

С согласия руководителя следственного органа постановление направляется в суд и в случае принятия судом решения о получения информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется в соответствующую организацию связи. Руководитель организации связи, куда было направлено решение суда, обязан предоставить интересующую следователя информацию[1].

Суть основного этапа заключается как в деятельности следователя, так и конкретного сотрудника организации мобильной связи. Данный этап также можно представить в виде двух относительно самостоятельных стадий.

Первая стадия касается технических мероприятий. После получения организацией связи постановления и копии судебного решения от следователя на производство следственного действия, предусмотренного ст. 186.1 УПК РФ, конкретный сотрудник в рамках своей компетенции и возможностей оборудования производит действия технического характера. Затем систематизирует и отправляет информацию следователю. Информация, поступающая от мобильного оператора, может быть зафиксирована на любом материальном носителе и предоставляется в опечатанном виде с сопроводительным письмом, в котором указывается период времени и номера абонентов или абонентских устройств[2].

Вторая стадия – исследовательская. Следователь, получив сведения от оператора, изучает и анализирует информа-

---

[1] Уголовно-процессуальный кодекс Российской Федерации. Ч. 3 ст. 186.1 (действующая редакция) [Электронный ресурс]. URL: http:/www.consultant.ru.

[2] Уголовно-процессуальный кодекс Российской Федерации. Ч. 3 ст. 186.1 (действующая редакция) [Электронный ресурс]. URL: http:/www.consultant.ru.

цию о соединениях между абонентами и (или) абонентскими устройствами, выполняет некоторые процессуальные действия, а также принимает ряд тактических решений, касающихся хода дальнейшего расследования. Полученные от оператора данные о соединениях следователь осматривает в присутствии понятых, а при необходимости – с участием специалиста, и в этот момент подробно описываются все технические действия, связанные с просмотром информации. Цель исследовательской стадии основного этапа – систематизировать представленный массив данных и осуществить выборку криминалистически значимой информации.

Заключительный этап характеризуется закреплением сведений, полученных от оператора связи, в качестве вещественного доказательства. Результатом осмотра является протокол осмотра документов, в котором, по мнению следователя, указывается наиболее значимая информация для уголовного дела. Другие участники данного следственного действия могут в этом же протоколе либо отдельно от него указать свои замечания. Данный протокол может быть составлен непосредственного после осмотра всего массива предоставленной информации либо по ходу ее изучения. Кроме того, следователь составляет постановление о признании и приобщении к уголовному делу вещественного доказательства, т. е. полученной детализации. Изученные материалы приобщаются в полном объеме на основании постановления следователя и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность. Особенность заключительного этапа – это наличие двух завершающих следственное действие документов.

По нашему мнению, соблюдение определенной тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами позволяет следователю решить задачи не только следственного действия, но и некоторые задачи расследования[1]. Сведения об абонентах и их соединениях, предоставляемые оператором сотовой связи, в рамках производства следственного действия, предусмотренного статьей 186.1 УПК РФ, нередко выступают в качестве одного из самых решающих доказательств по уголовному делу. Располагая данной информацией, следователь может продемонстрировать осведомленность по поводу

[1] *Дерюгин Р. А.* Тактические особенности производства следственного действия, предусмотренного ст. 186.1 Уголовно-процессуального кодекса РФ // Электронное приложение к «Российскому юридическому журналу». 2017. № 1. С. 22.

события преступления, фактов, связанных с лицами, причастными к преступному событию, оперируя при этом конкретными контактами, датой, длительностью переговоров, частотой вызовов, а также примерным местонахождением абонентских устройств во время разговоров.

Несмотря на вышесказанное, следует отметить, что тактика рассматриваемого следственного действия лишь постепенно нарабатывается, но уже сейчас важно обеспечить правоприменителя криминалистическими рекомендациями, направленными на повышение результативности следственного действия, минимизации процессуальных ошибок и потенциально конфликтных ситуаций расследования.

Правовые и организационные вопросы обеспечения безопасности в условиях развития информационного общества

Е. Е. Кошелева,
старший участковый уполномоченный полиции (УМВД России по г. Дзержинску)

В статье рассматриваются некоторые вопросы обеспечения информационной безопасности в условиях глобализации современного общества; делается определенный вывод о том, что наше государство стоит на пороге очередного витка гонки вооружений, существует опасность развязывания глобальной информационной войны.

Информация, информационные технологии, информационная война, безопасность, информационная безопасность.

Наступившее столетие ярко демонстрирует стремительное развитие высоких технологий. Это стало отчетливо заметно в конце XX – начале XXI в. Именно этот период ознаменовал собою стремительное развитие кибернетических технологий, резкое увеличение объемов влияния глобальной информационно-телекоммуникационной сети Интернет, всеохватность информационных потоков и глобализацию информационных процессов. Одной из основных движущих сил развития общества и экономики стала информация, в том числе и компьютерная. Но в рамках информатизации, одновременно с прогрессом, наблюдается и рост преступности в сфере информационной безопасности.

Нарастающее развитие информационных технологий предполагает, с одной стороны, улучшение качества жизни общества, с другой – совершенствование механизмов подготовки, совершения и сокрытия преступлений в сфере информационной безопасности[1].

Преступники становятся все более технологически оснащенными, подготовленными и информационно осведомленными. Это, в свою очередь, прямо способствует развитию преступности в данной сфере, в том числе и транснациональной.

[1] *Репин М. Е.* Личность «компьютерного преступника» в контексте криминалистической характеристики преступлений в сфере компьютерной информации // Криминалистические средства обеспечения деятельности по выявлению и расследованию преступлений экономической и коррупционной направленности: сборник статей / [под ред. А. Ф. Лубина]. Казань, изд-во «Бук», 2017. С. 194–196.

Небывалое возрастание значения информации и ее роли в жизни общества в условиях глобализации еще в начале XX в. предусматривал немецкий философ Шпенглер. В работе «Закат Европы» он писал: «В ближайшем будущем три или четыре мировых газеты будут направлять мысли провинциальных газет и с их помощью – «волю народа». Все будет решаться небольшим количеством людей, контролирующих эти газеты, имена которых, возможно, даже и не будут известны, однако огромная масса политиков второго ранга, риторов и трибунов, депутатов и журналистов, представителей провинциальных горизонтов будет поддерживать в низших прослойках общества иллюзию народного самоопределения»[1].

Средства массовой информации, как составляющая часть современной информационно-коммуникационный и культурной сферы жизнедеятельности общества и государства, всегда были и будут активными участниками различных вооруженных войн и конфликтов. Весьма символически, на наш взгляд, выглядит факт, ставший 60 лет назад поводом для Второй мировой войны, – нападение на радиостанцию в Глейвице. Многие великие историки отмечают, что Б. Муссолини, по мнению его же соратников, при планировании военных операций больше внимания уделял тому, какие заголовки появятся в газетах и книгах, а также других средствах массовой информации, чем воинской доктрине, мудрости и целесообразности. Однако, как мы видим, именно те страны и государства, у которых достижения в информационно-пропагандистской сфере были наиболее яркими и убедительными, испытали поражение и неудачу во Второй мировой войне[2]. С течением времени комплекс мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им определенных целей, которые не входят в число их взглядов и интересов, а также защиту от подобных воздействий получил определение «информационная война»[3].

Информационная война в отношении Российской Федерации, следует отметить, велась и ведется постоянно. Временами с меньшей или большей активностью и эффективностью. Как всем нам хорошо видно, наше время не является каким-либо исключением из сложившейся ситуации в мировом геополитическом пространстве.

---

[1] *Шпенглер О.* Закат Европы. М.: издательство «Эксмо», 2006. С. 230.

[2] *Гриняев С. Н.* Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Минск: Харвест, 2004. С. 187.

[3] *Манойло А. В.* Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта // Пси-фактор [Электронный ресурс]. URL: http://psyfactor.org/lib/psywar35.htm (дата обращения: 24.03.2018).

Уже на наших глазах и с нашего попустительства в информационном поле русских, живущих на национальных окраинах исторической России, в Киргизстане, Казахстане, Прибалтике, перестали называть, а соответственно и считать русскими. Их именуют теперь «киргизстанцы», «казахстанцы», «прибалтийцы», а общее обозначение – русскоязычные. Русских же, живущих в России, теперь именуют россиянами. Теперь мы вынуждены констатировать – это не простая игра слов и выражений в суете глобализации мирового пространства, не невинная перетасовка имен. Племенное имя для нации, пусть даже и разделенной, есть залог будущего воссоединения и единства. Это великолепно знают и отчетливо понимают идеологи и пропагандисты информационной войны. Да и нам, в отношении кого идет данная война, необходимо это понимать и осознавать. И, конечно, бороться с этим всеми легитимными способами[1].

Мы понимаем, что все это вынуждает нас признать необходимым ведение своей собственной специальной государственной пропаганды и политики в сфере кибернетической безопасности и информационных технологий. Все необходимые ресурсы для этих целей у нас имеются. Только по самым скромным подсчетам, на территории Украины и Прибалтики 20 % общего населения причисляют себя к русской нации и исповедуют единые интересы. Данная социальная масса, бесспорно, представляет собой мощнейшую силу. При ее грамотном, умелом и своевременном использовании появляется возможность нейтрализации агрессивной политики со стороны соседних государств и лоббирования собственных интересов. Ярким примером могут являться массовые демонстрации в Прибалтике со стороны русского населения, прошедшие после принятия решения о переносе памятника воинам, погибшим во время Второй мировой войны[2]. Тогда органы государственной власти соответствующих государств с огромным трудом смогли справиться с нарастающим протестом. При этом активное участие в них приняло около 60 % русского населения. Тем самым при активности подавляющего большинства русского населения местной власти пришлось бы пойти на более существенные уступки, вплоть до изменения стратегии национальной политики.

Известный журналист и научный работник Гриняев Сергей отмечает: до недавнего времени в Российской Федерации практиче-

---

[1] *Долинко В. И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

[2] Эстонская действительность: сегодняшние реалии [Электронный ресурс]. URL: http://www.estonia-today.narod.ru/ (дата обращения: 14.04.2018).

ски не существовало единой государственной позиции по актуальным вопросам информационной безопасности. Это, по его мнению, и привело к поражению в холодной информационной войне[1]. Только в декабре 2016 г. Президентом России была подписана Доктрина информационной безопасности России, в которой стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности[2]. Для реализации стратегических положений Доктрины и обеспечения информационной безопасности нашей страны было создано Управление информационной безопасности в Совете Безопасности России, которое координирует действия ФСБ, ФСО, ФАПСИ, Министерства обороны и МВД России[3].

Проведенный анализ складывающейся в современном мире ситуации показал, что многие страны мира сейчас создают у себя системы защиты от американской культурной экспансии и информационной агрессии. В той же Италии, например, по телевидению разрешается показывать не более 40 % иностранных фильмов и передач, абсолютное большинство которых, как известно, американские. Данный опыт может быть применен в охране и защите прав и законных интересов своих собственных граждан. Для обеспечения безопасности Российской Федерации, учитывая сложность и специфичность информационного воздействия, жизненно необходим специальный координационный управляющий орган по контролю за созданием, хранением и применением «информационного оружия». Также необходимо создание единого межведомственного аналитического центра по разработке новейших информационно-

---

[1] См.: *Гриняев С.* Информационная война: история, день сегодняшний и перспектива. М.: издательство «Прогресс», 2006. С. 78.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. // Рос. газ. 2016. 6 дек.

[3] *Афанасьев А. Ю., Репин М. Е.* Уголовно-процессуальные и криминалистические особенности расследования киберпреступлений // Криминалистическое обеспечение раскрытия и расследования преступлений: материалы X всероссийского научно-практического круглого стола (Ставрополь, 26 февраля 2016 г.). Том 1. Ставрополь, 2016. С. 12–13.

психологических технологий на базе МВД России или ФСБ России при возможном патронаже Совета Безопасности России.

Складывающаяся в мировом пространстве геополитическая ситуация наставляет нас задуматься о создании и функционировании мощного единого государственного холдинга средств массовой информации (масс-медиа), действующего в непосредственном взаимодействии со специалистами из информационно-аналитического центра. С целью обеспечения информационной безопасности и решения проблем информационной войны, а также для качественной подготовки журналистов «нового типа», формирования у них необходимой профессиональной компетенции, следует приложить совместные усилия для того, чтобы в XXI столетии достижения в области кибернетики и информационных технологий служили исключительно на благо всего человечества нашей планеты.

К сожалению, в современных условиях всеобщей глобализации и интеграции это направление до сих пор остается недостаточно изученным и разработанным. Ему не уделяется должного внимания со стороны ученых и политиков. Вместе с тем, одной из важнейших и первостепенных задач можно и нужно считать решение существующих проблем в рассматриваемой сфере. Так, упустив момент сегодня, мы рискуем уже завтра встать на порог очередного витка смертельно опасной гонки вооружений. В этом случае опасность развязывания глобальных информационно-телекоммуникационного противодействия и войны, объектом воздействия в которых станет самое утонченное достижение мировой эволюции – сознание человека, станет самой жестокой и суровой реальностью.

Отдельные аспекты применения современных инновационных технологий в раскрытии и расследовании преступлений

Т. А. Кулибаев,
доктор юридических наук, профессор
(Алматинская академия МВД
Республики Казахстан им. М. Есбулатова)

В статье обосновывается необходимость применения современных инновационных технологий в деятельности правоохранительных органов Республики Казахстан, анализируется опыт применения программно-аппаратных комплексов и определяется направление дальнейшего развития в данной сфере.

Информатизация, расследование преступлений, криминалистическая техника, уголовное судопроизводство.

Эффективность как эмпирического (опытного), так и теоретического познания во многом зависит от того, насколько в нем определены предмет и задачи исследования. Это актуально и для такой формы познания, как раскрытие и расследование преступления. Наряду с этим в рамках первоначальных действий стоит задача закрепления доказательств, которые в последующем могут лечь в основу обвинения, либо же стать исходными данными или предметом экспертного исследования.

В Послании Главы государства Н. Назарбаева народу Казахстана «Новые возможности развития в условиях четвертой промышленной революции» от 10 января 2018 г., изложено: «...важной является цифровизация процессов в госорганах, включая их взаимодействие с населением и бизнесом в сфере охраны общественного порядка и обеспечения безопасности нужно активно внедрять интеллектуальные системы»[1].

В связи с этим повышение эффективности работы правоохранительных органов на современном этапе развития общества невоз-

[1] Послание Президента Республики Казахстан – Лидера нации Н. А. Назарбаева народу Казахстана от 10 января 2018 г.: «Новые возможности развития в условиях четвертой промышленной революции» // URL:http://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-prezidenta-respubliki-kazahstan-n-nazarbaeva-narodu-kazahstana-10-yanvarya-2018-g (дата обращения: 10.03.2018).

можно без интеграции в правоохранительную сферу новых инновационных технологий.

Эволюция современного общества, а также анализ современной практики противодействия преступности в Казахстане убедительно свидетельствует о том, что эффективность этой деятельности напрямую зависит от применяемых средств и методов. Их соответствие новейшим достижениям науки и техники предопределяет успешное решение задач борьбы с преступностью.

В силу этого использование научно обоснованных методов в сфере информационного обеспечения и информационного взаимодействия является первостепенной проблемой правоохранительной деятельности. Фактически весь процесс раскрытия и расследования преступлений носит ярко выраженный информационный характер. В содержательном аспекте деятельность по информационному обеспечению и информационному взаимодействию в ходе досудебного расследования представляет собой последовательный процесс познания события и признаков преступления.

Следует учитывать, что достижения в области наукоемких технологий используют и современные преступники для совершения преступлений, относящихся к разряду трудно раскрываемых. Так, например, интернет способствует таким видам деятельности, как террористические акты, интеллектуальные угрозы, вторжение в различные (общедоступные, частные, коммерческие и др.) сети для нарушения процесса их функционирования. Уязвимость государственных, коммерческих, частных структур от подобного рода преступной деятельности объясняется тем, что критически важные объекты инфраструктуры становятся все более зависимыми от взаимосвязанных компьютерных сетей и всемирной паутины[1]. Каждое преступление непременно отражается во внешней окружающей среде в качестве материальных следов либо в форме образов в человеческом сознании, в силу чего может рассматриваться в качестве информации. Вопросы, касающиеся возможных путей получения, фиксации, преобразования, передачи, искажения и утраты информации, ее исследования и оценки, являются особо актуальными для методологии расследования преступлений. Недостаток информации, трудности в информационном взаимодействии между различными подразделениями или ведомствами создают существенные препятствия для успешной деятельности правоохранительных органов.

---

[1] *Дильбарханова Ж. Р.* Использование инновационных технологий в преступных целях, предупреждению и борьбе с преступностью // Материалы Международной научно-практической конференции «Современное уголовное законодательство: проблемы, тенденции и пути модернизации». Алматы: Казак университеті, 2013.

Современное криминалистическое обеспечение процесса раскрытия преступлений невозможно представить без специальной техники, используемой для исследования доказательств и получения необходимой информации для быстрого и полного их раскрытия. Весьма важную роль в данном вопросе играет высокий уровень технико-криминалистического сопровождения данной деятельности.

Вместе с тем, так было не всегда. Первоначально использование техники при получении информации, имеющей значимость для расследования уголовного дела, носило фрагментарный характер, исследовались лишь отдельные аспекты прикладного характера, связанные с использованием единичных технических средств, например средств фотографии.

Термин «научная техника расследования преступлений» был введен в научный оборот профессором Лозаннского университета Р. Рейссом. Этим термином предлагалось обозначать применение научных методов исследования преступлений[1]. Это понятие использовалось для обозначения совокупности научных методов, способов и приемов, используемых для раскрытия и расследования преступлений.

Слово «техника» достаточно широко используется в современной теории уголовно-процессуального права, криминалистики. Например, техника доказывания, криминалистическая техника и т. п. По мнению А. А. Кухты, техника доказывания включает в себя, во-первых, представление и исследование фактов, а, во-вторых, встраивание этих фактов в систему аргументации, само аргументирование и, наконец, инсталляцию частного знания, содержащегося в приговоре суда, в общую систему знания, существующего в данной дискурсивной формации. Технику доказывания можно трактовать и как умение пользоваться фактами и презумпциями[2].

М. С. Строгович, рассуждая о предмете науки криминалистики, отмечал, что, прежде всего, «криминалистика изучает научно-технические приемы собирания и исследования доказательств. В своем конкретном содержании наука криминалистики строилась до сих пор почти исключительно применительно к условиям расследования уголовных преступлений и сводилась к сумме научно-техниче-

---

[1] *Рейсс Р. А.* Научная техника расследования преступлений. Курс лекций, прочтенных в г. Лозанне профессором Рейссом чинам русского судебного ведомства летом 1911 года. СПб., 1912.

[2] *Кухта А. А.* Юридическая техника и техника доказывания по уголовным делам // Юридическая техника. Н. Новгород, 2007. № 1.

ских методов следствия...»[1]. Здесь речь фактически идет о разделе криминалистики, именуемом в современной литературе криминалистической техникой.

Впервые исследование собственно научно-технических средств было произведено Н. А. Селивановым. Им было предложено использовать понятие научно-технических средств в двух смыслах: в узком и широком. Так, «под научно-техническими средствами в узком смысле понимаются приборы, инструменты, различного рода приспособления и материалы, так или иначе способствующие решению задач уголовного судопроизводства путем их применения для обнаружения, фиксации, изъятия и исследования доказательств, фиксации хода и результатов следственных и судебных действий, а также предупреждения преступлений. В широком же смысле данное понятие включает также методы (способы, приемы) и методики применения технических средств»[2].

Криминалистическая деятельность в вопросах раскрытия и расследования преступлений, а также уголовно-процессуальное судопроизводство немыслимо без использования в своем арсенале современных достижений научно-технического прогресса, которые находят свое отражение в форме научно-технических средств. В связи с этим на законодательном уровне необходимо регулировать правоотношения, связанные с применением научно-технических средств, например с применением полиграфа.

Н. К. Имангалиев под научно-техническими средствами понимает «любые технические средства и научные методы, используемые в установленном законом порядке для обнаружения, фиксации, исследования, моделирования, проверки и демонстрации доказательств, а также направленные на повышение эффективности деятельности органов, ведущих уголовный процесс, и установление обстоятельств, имеющих значение для правильного разрешения уголовного дела»[3].

Для эффективного применения научно-технических средств, а главное для решения задач уголовного судопроизводства должны быть соблюдены требования их использования. Анализ норм уголовно-процессуального кодекса РК приводит к выводу о том, что требования к научно-техническим средствам для получения кри-

---

[1] *Строгович М. С.* Уголовный процесс. М., 1940.

[2] *Селиванов Н. А.* Научно-технические средства расследования преступлений: автореф. дис. ... д-ра.юрид. наук. М., 1965.

[3] *Имангалиев Н. К.* Научно-технические средства при расследовании преступлений: теория и практика применения: автореф. дис. ... к. ю. н. Караганда, 2010.

миналистически значимой информации едины для всех стадий уголовного судопроизводства.

Значение уголовно-процессуальной формы использования научно-технических средств при получении криминалистически значимой информации, необходимой для выявления, раскрытия и расследования преступлений, в том числе в доказывании по уголовным делам, состоит в том, что они обеспечивают всесторонность, полноту и объективность исследования обстоятельств, подлежащих доказыванию по уголовному делу, повышают достоверность результатов произведенных следственных и судебных действий, а также способствуют реализации процессуальных гарантий, законных прав и интересов участников уголовного судопроизводства, к которым может быть отнесено право обладателя информации на копирование данных с изымаемых при производстве следственных действий носителей информации. Получение криминалистически значимой информации может происходить как в рамках уголовно-процессуальной формы, так и за ее пределами, например при осуществлении оперативно-розыскной деятельности и других видов правоохранительной деятельности. Однако доказательства могут собираться лишь в уголовном судопроизводстве, в ходе же оперативно-розыскных мероприятий могут быть получены лишь материалы, содержащие следы преступления. Поступив к следователю, эти материалы или результаты оперативно-розыскной деятельности осматриваются, устанавливается относимость сведений об их свойствах и состояниях, составляется протокол следственного действия. Допустимость доказательства при этом обеспечивается соблюдением условий и порядка производства следственного действия.

В отличие от отдельных правил, которыми могут регламентироваться особенности использования научно-технических средств (время начала и окончания записи, указание кратких характеристик технических средств, использованных при производстве следственного действия, предусмотренное ч. 6 ст. 197 УПК РК), требования, предъявляемые к использованию научно-технических средств, формулируют наиболее общие, сущностные, принципиальные положения, определяющие условия и порядок их использования. При проведении следственных действий, предусмотренных конкретно поименованными статьями УПК РК, привлечение понятых обязательно. В остальных случаях при проведении следственных действий в обязательном порядке применяются научно-технические средства фиксации хода и результатов. В случае отсутствия научно-технических средств или невозможности их применения при проведении следственных действий привлекаются понятые. Такие требования УПК РК являются проявлением принципов уголовного

судопроизводства, носящих более общий характер. Представляется, что в число рассматриваемых требований должны быть включены: законность, этичность, научность, безопасность, обоснованность и эффективность. Такое законодательное закрепление будет способствовать единообразному пониманию их правоприменителем.

В настоящее время в деятельности правоохранительных органов Республики Казахстан активно применяются новые инновационные технологии. Их использование во всех их проявлениях всегда было в центре основных дискуссий борьбы с преступностью.

Сегодня существуют несколько самостоятельных информационных систем:

– оперативные учеты,

– системы оперативно-розыскной информации;

– банки вспомогательных данных, направленные на решение задачи обеспечения процесса раскрытия и расследования преступлений необходимой информацией (о лицах, которые совершили или могли совершить преступление либо причастны к нему; о нераскрытых преступлениях; о принадлежности обнаруженных вещественных доказательствах, в первую очередь различных видов материальных следов).

Информационные системы способны решать различные задачи. Две из которых нам представляются наиболее важными.

1. Информационные – такие, когда с помощью накопленных данных осуществляется идентификация конкретных криминалистических объектов.

2. Розыскные – предполагающие содействие розыску лиц и объектов, информация о которых содержится в оперативных учетах, информационных системах оперативно-тактического назначения. Решение розыскных задач тесно связано с распознаванием образов криминалистических объектов, то есть диагностикой.

Постоянно увеличивающийся поток информации, который необходимо оперативно и своевременно обрабатывать, требует внедрения новейших автоматизированных программ. В 2000 г. был создан и введен в действие АПК ЦОУ. В работе центра используются передовые компьютерные технологии, научные рекомендации и достижения технического прогресса. В разработанной структуре ЦОУ реализованы лучшие наработки по оперативному реагированию полиции зарубежных стран с высоким уровнем преступности. Кроме того, в целях повышения эффективности работы оперативно-справочных учетов созданы автоматизированные учеты: в рамках проекта разработан и внедрен программно-технический комплекс АИС «Автоматизированная дактилоскопическая информационная

система» («АДИС») – «Папилон», обеспечивающий: ведение автоматизированного банка данных дактилоскопической информации. Практика последних лет убедительно доказала высокую эффективность и громадную практическую отдачу от внедрения компьютерных систем автоматизации дактилоскопических учетов.

Кроме того, проведена работа по автоматизации видео- и фотоучетов, внедрены современные технологии автоматизированного поиска лиц по базам данных фотоизображений. Это продукт отечественных разработчиков АИПС «Образ ++». Усовершенствованная система «Образ ++», характеризующаяся высокой точностью и скоростью поиска данных по портрету лица, а также устойчивостью качественных характеристик портретного поиска при внешних изменениях одного и того же лица, позволяет проводить портретную идентификацию путем автоматического поиска и сравнения фотографического изображения с максимальной степенью сходства из базы данных АИПС с фотографией сравниваемого лица, введенной через сканер. Базы данных, заполняемые в различных подразделениях ОВД, объединяются для пополнения массива и создания единого банка данных.

Вышеизложенное свидетельствует о том, что в последние годы в нашей стране началось интенсивное внедрение и использование в общественной деятельности перспективных информационных технологий, проникающих во все сферы социально-экономической жизни. Инновационные достижения обеспечивают определенный прорыв в вопросах борьбы с преступностью и требуют ведения новелл в уголовный процесс. Для того, чтобы теоретическая возможность использования научно-технических достижений стала практической реальностью, нужны большие организационные усилия.

Эффективное информационное обеспечение может быть реализовано только в ходе информатизации органов досудебного расследования в системе МВД Республики Казахстан. Существующие сегодня информационно-коммуникационные технологии нуждаются в дальнейшем совершенствовании, направленном на их глобализацию, расширение доступа и количества информационных функций, направленных на решение задач борьбы с преступностью. Эта задача может и должна быть решена силами научно-исследовательских центров, действующих в системе МВД Республики Казахстан.

Кроме того, такие новшества должны быть поддержаны правовым путем, сопровождаются привлечением современных программных средств и технологий, что, на наш взгляд, позволит сократить временные затраты сотрудников оперативных и следственных подразделений, сроки расследования уголовных дел, а также повысить качество и уровень расследования.

Организация использования возможностей сети Интернет при раскрытии преступлений

А. Ф. Купин,
доцент кафедры,
кандидат юридических наук
(МГТУ им. Н. Э. Баумана)

А. А. Павлова
(МГТУ им. Н. Э. Баумана)

В статье рассматриваются возможности применения ряда программных продуктов и поисковых систем для решения задач по распознаванию неизвестных лиц и предметов с помощью сети Интернет. На основании проведенного анализа функциональных возможностей этих программных продуктов и технических средств делается вывод о необходимости их использования для решения задач криминалистики.

Распознавание лиц и предметов, программные средства, поисковые системы.

Развитие любых сфер деятельности современного общества сегодня связано с использованием сети Интернет. В основном ее возможности применяются для поиска необходимой информации. Сравнительно недавно пользователям сети Интернет поиск информации был доступен лишь с помощью ключевых слов, введенных в поисковой строке браузера. Однако с развитием технологий искусственного интеллекта была реализована возможность поиска данных по загруженному изображению объекта. Несмотря на то, что развитие технологий поиска в сети Интернет предназначено прежде всего для решения повседневных задач, не связанных с криминалистической деятельностью (выбор понравившегося товара, образовательная деятельность и т. д.), ресурсы сети Интернет могут представлять ценность и для решения ряда задач криминалистики, например, задачи по поиску и распознаванию лиц и предметов по их изображениям. Остановимся подробнее на возможностях некоторых программных средств, которые могут применяться правоохранительными органами для решения поставленных перед ними задач по розыску лиц и предметов[1].

[1] *Яковлева А. В., Алабердеев Р. Р., Андросов С. М., Афицинский В. А., Бабак Ю. Н., Баширова Н. В., Беспалько А. А., Бойко М. В., Бурбело О. А., Быкова К. В., Гапоненко А. В.,*

В поисковую систему «Яндекс» функция поиска объектов по их изображению была введена в 2013 г. посредством реализации технологии компьютерного зрения «Сибирь». В основу этой технологии положен специальный алгоритм, позволяющий разбивать загруженную картинку на «визуальные слова» – численные представления ключевых элементов изображения, что позволяет сопоставлять эту картинку с миллиардами известных изображений, содержащих такие же «визуальные слова», отсекая все остальные. Такой подход позволяет обнаруживать копии изображения как с аналогичными размерными характеристиками, так и с другими размерами. В настоящее время создана и успешно функционирует усовершенствованная версия технологии «Сибирь», которая позволяет, используя опцию «Яндекс- Картинки», найти не только копии, но и похожие фотоснимки загруженного изображения[1]. Для ее максимально успешного применения необходимо на изображении выделить область, содержащую искомый объект путем удаления (обрезки) лишних элементов фотоснимка. В противном же случае результаты поиска станут менее эффективными, так как будут определяться предметы, имеющие схожую форму и (или) цветовой тон, но, как правило, не относящиеся к типу и виду исследуемого предмета. Для проверки работы указанной технологии нами был проведен эксперимент, который подтвердил возможности поиска изображений предметов подобным образом. Так, при загрузке изображения неопознанного предмета, в качестве которого использовался фрагмент разрезанной упаковки «Bertie Botts Beans», было найдено изображение целой упаковки «Bertie Botts Beans».

Поиск предметов по их изображению в системе Интернет может быть реализован и с помощью поисковой системы «Google». Так, при загрузке изображения в поисковой строке системы «Google» автоматически определяется категория, к которой относится искомый объект. С целью проверки поисковых возможностей данной системы нами был осуществлен с ее помощью поиск неопознанного предмета, в качестве которого также использовалось изображение разрезанной упаковки «Bertie Botts Beans». При этом поисковой системой «Google» была максимально точно определена категория изображенного предмета – «Bertie Botts Every Flavor Beans». Менее эффективный результат был показан при загрузке для поиска в качестве

Гассий В. В., Герасимов А. В., Головко М. В., Долинко В. И., Еськов С. В., Злобина И. В., Калинина Н. Н., Камкия Б. А., Кизим А. А. и др.: Механизм экономико-правового обеспечения национальной безопасности: опыт, проблемы, перспективы. Краснодар, 2012.

[1] Яндекс. Яндекс научился искать без слов. URL: https://yandex.ru/blog/company/71302 (дата обращения: 22.04.2018).

неопознанного предмета фотоснимка термовоздушной паяльной станции. В результате поиска загруженного изображения указанного предмета аналогичных изображений подобных предметов в сети Интернет найдено не было. Однако при этом во вкладке «Страницы с похожими изображениями» отобразились ссылки на страницы сети Интернет, содержащие изображение данного объекта.

Возможности поисковой системы «Bing» также позволяют решать задачи поиска объектов по их изображению. Так, например, с ее помощью поиск загруженного изображения термовоздушной паяльной станции оказался результативным: было найдено изображение предмета, аналогичное искомому. Существенным преимуществом поисковой системы «Bing», по сравнению с иными, является то, что в нее встроена функция выделения части изображения, позволяющая дифференцировать поиск изображения по его отдельным фрагментам, без использования дополнительных средств и приемов, например, графических редакторов.

Поиск объектов по их изображению в сети Интернет может быть проведен и с использованием приложений для мобильных устройств. Одним из таких программных продуктов является приложение «Reversee». Бесплатная версия данного приложения позволяет загрузить имеющееся в памяти мобильного устройства изображение (сфотографированное самостоятельно либо предоставленное другим пользователем) в сеть Интернет и затем осуществить поиск сходных с ним изображений с помощью поисковой системы «Google». Платная версия приложения «Reversee» предоставляет дополнительные возможности поиска искомого изображения с использованием ресурсов систем «Yandex» и «Bing». В настоящее время описанная технология поиска позволяет эффективно находить изображения предметов и проверяемых лиц при наличии их полных изображений, а также, в ряде случаев, при направлении на поиск отдельных фрагментов изображений.

Эффективным средством поиска изображений лиц, размещенных в сети Интернет, является приложение «TinEye», созданное канадской компанией «Idee Inc». Используя систему «MatchEngine», которая работает со своей собственной коллекцией изображений, указанное приложение находит похожие или повторяющиеся версии загруженного ранее и сохраненного фотоснимка[1].

Поскольку значительное количество изображений лиц содержится в социальных сетях, то эффективный поиск возможен

[1] Tin Eye. MatchEngine. URL: https://services.tineye.com/MatchEngine#how-it-works (дата обращения: 22.04.2018).

с использованием специальных приложений, созданных под конкретные социальные сети. Например, для анализа изображений лиц в социальной сети «ВКонтакте» в феврале 2016 г. компания «N-Tech Lab» создала программное средство «FindFace», которое по результатам конкурса «Megaface», организованного университетом Washington, обошло по своей эффективности программное обеспечение распознавания «Google»[1]. Возможности его практического применения достаточны просты. Для использования данного ресурса необходимо авторизоваться в социальной сети «ВКонтакте» и загрузить изображение лица, после чего программа осуществит поиск по базе находящихся изображений.

Следует отметить, что описанные выше приложения не производят идентификационное сравнительное исследование обнаруживаемых изображений. Наряду с ними для осуществления поиска лиц по их изображению в сети Интернет могут применяться и иные программные продукты. Например, такие приложения, как «VOCORD FaceMatica», проводящее сравнение лиц, изображенных на разных снимках[2], «FaceRect», анализирующее более 100 параметров точек загруженного изображения лица и представляющее вывод «JSON-файла», содержащего вектор ориентиров лица (глаз, носа, рта)[3] и ряд других.

Обобщая вышеизложенное, отметим, что на сегодняшний день разработано множество программных средств, созданных для поиска и идентификации лиц и предметов по их изображениям, путем анализа данных, выложенных в сети Интернет. Анализ результатов, полученных при использовании различных программных средств для поиска лиц и предметов по их изображениям, свидетельствуют о том, что у каждого программного продукта есть свои преимущества. Так, с помощью поисковой системы «ЯндексКартинки» представляется возможным определить предмет по изображению его фрагмента, поисковая система «Bing» наилучшим образом проводит поиск фотоснимков предметов с отсутствующими маркировочными обозначениями, а технология поисковой системы «Google» при успешном распознавании изображенного объекта отсеивает максимальное количество изображений, не относящихся к типу искомого предмета. В свою очередь мобильное приложение «Reversee»

---

[1] FindFace.Pro. URL: https://findface.pro/ru/ (дата обращения: 22.04.2018).

[2] Vocord FaceMatica. URL: http://vocord.ru/facematica/ (дата обращения: 22.04.2018).

[3] FaceRect API. URL: http://apicloud.me/apis/facerect/demo/ (дата обращения: 22.04.2018).

позволяет определить зафиксированный на изображении предмет, анализируя данные через поисковые системы «Google», «Yandex» и «Bing». Система поиска «TinEye» наиболее рациональна для поиска изображений лиц, выложенных в сети Интернет, а программный продукт «FindFace» специализирован на поиске изображений лица путем анализа профилей пользователей социальной сети «ВКонтакте». Для получения эффективного результата по поиску лиц и предметов по их изображениям, как правило, необходимо комплексное использование программных средств с учетом их специфических возможностей, временных рамок и характера решаемых в ходе поиска задач.

Ситуационные центры как инструмент раскрытия, расследования и профилактики преступлений в сфере высоких технологий

Н. В. Лукашов,
ведущий научный сотрудник,
кандидат физико-математических наук, доцент
(Академия управления МВД России)

В статье рассматриваются проблемы организации раскрытия и расследования преступлений в сфере высоких технологий.

Организация, раскрытие преступлений, расследование преступлений, преступления в сфере высоких технологий.

Термин «высокие технологии» (ВТ) все более активно используется в правоохранительной деятельности. Это обусловлено в первую очередь технологическим развитием общества. Считается, что данный термин «сложился стихийно» и употребляется «для удобства обозначения преступлений, орудием или предметов которых стала компьютерная информация или компьютерные средства»[1]. Между тем такая трактовка ВТ как синонима информационным компьютерным технологиям (ИКТ), на наш взгляд, не вполне корректна, поскольку представляет ВС в узком смысле, не учитывая остальных сложных технологических отраслей.

Это отражается и в нормативных правовых актах (НПА) правоохранительных органов. Например, информационное обеспечение сотрудничества по линии Интерпола, регламентированное соответствующей Инструкцией[2], предусматривает направление запросов «о преступлениях в области *высоких технологий*». При этом под ВТ подразумеваются лишь связанные: с «неправомерным доступом к компьютерной информации»; «созданием, использованием и распространением вредоносных программ для ЭВМ»; «нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети». Таким образом, упомянутая Инструкция ограничивает ВТ сферой ИТ.

---

[1] *Кушниренко С. П.* Методика расследования преступлений в сфере высоких технологий. СПб., 2007. С. 3.

[2] Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ от 6 октября 2006 г. МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 (ред. от 22.09.2009).

УК РФ также не содержит статей, предусматривающих ответственность за совершение преступлений в сфере ВТ, ограничиваясь главой 28 «Преступления в сфере компьютерной информации».

Между тем вне сферы правоохранительной деятельности ВТ трактуются значительно шире. Например, как *«совокупность информации, знаний, опыта, материальных средств, используемых при разработке, создании и производстве как новых (ранее неизвестных) продукций и процессов, так и для улучшения качества и удешевления производства известных продуктов»*[1]. Таким образом, к ВТ можно отнести, например, генетические, космические, ядерные, нано и ряд других технологий, непосредственно относящихся к ИТ.

Другой пример: программой создания технопарков «в сфере высоких технологий» предполагается приоритетное развитие таких «высокотехнологичных отраслей экономики», как «энергоэффективность и энергосбережение (в том числе разработка новых видов топлива), космические технологии (в том числе связанные с телекоммуникациями – ГЛОНАСС и наземная инфраструктура), медицинские технологии»[2]. Очевидно расхождение между правовой и общепринятой терминологией в форме сужения общего понятия ВТ до ИТ.

При этом общей методике расследования преступлений в сфере ВТ, на наш взгляд, не уделяется должного внимания. Между тем особенностью расследования таких преступлений является общая со сферой ИТ[3] необходимость привлечения специалистов, а также экспертов зачастую в достаточно редких областях знаний. Кроме того, повышаются требования к уровню межведомственного взаимодействия. Другим общим признаком преступлений в сфере ВТ является их повышенная общественная опасность, а также «инновационность», обусловленная неизвестными ранее схемами совершения преступлений, новизной самих технологий.

В указанных обстоятельствах традиционные методы расследования преступлений могут быть недостаточно эффективными. В пользу этого утверждения свидетельствует статистика. Так, соотношение числа зарегистрированных преступлений по ст.159.6 УК

---

[1] БРЭ: Научное издательство «Большая Российская энциклопедия»: в 30 т. М., 2006. Т. 6. С. 767.

[2] О государственной программе «Создание в Российской Федерации технопарков в сфере высоких технологий»: распоряжение Правительства РФ от 10 марта 2006 г. № 328-р (ред. от 29.11.2014).

[3] Криминалистика: учебник для студентов вузов, обучающихся по спец. «Юриспруденция» / Т. В. Аверьянова [и др.]. 4-е изд., перераб. и доп. М. : НОРМА : ИНФРА-М, 2013. С. 915.

РФ (мошенничество в сфере компьютерной информации) к количеству выявленных лиц, их совершивших, составляло: в 2013 г. – 1:8; 2014 г. – 1:7; 2015 г. – 1:25; 2016 г. – 1:19; 2017 г. – 1:10. В истекшем 2017 г. на 2 195 выявленных преступлений указанной категории пришлось 2 134, по которым уголовные дела были приостановлены (таблица № 1).

Таблица № 1.

Результаты противодействия преступности в сфере ИКТ

Преступление	2013 г.	2014 г.	2015 г.	2016 г.	2017 г.
Мошенничество в сфере компьютерной информации(ст.159.6 УК РФ): зарегистрировано/расследовано/направлено в суд/ приостановлено по ч.1 ст. 208 УПК РФ (п. 1; п. 2; п. 3; п. 4)/ выявлено лиц, совершивших преступления	693/ 215/ 192/ (405; 0;0;0) 93	995/ 266/ 237/ (558; 3;0;0) 135	5 443/ 409/ 282/ (4 263; 3;1;0) 219	4 329/ 354/ 284/ (4 200; 21;0;4) 234	2 195/ 209/ 172/ (2 132; 2;3;0) 213
Преступления в сфере компьютерной информации (ст. 272, 273, 274 УК РФ суммарно): расследовано/ направлено в суд/ приостановлено по ч. 1 ст. 208 УПК РФ (п. 1; п. 2; п. 3; п. 4) / выявлено лиц, совершивших преступления	2 563/ 2 301/ 2 082/ (269; 0;0;0) 632	1 739/ 1 321/ 1 114/ (321; 12;1;3) 560	2 382/ 1 213/ 1 023/ (530; 6;7;4) 3 360	1 748/ 903/ 754/ (762; 25;3;1) 467	1 883/ 726/ 526/ (1 019; 7;5;0) 494

Учитывая достаточно высокую латентность преступлений в сфере ИКТ[1], а также ВТ в целом, вопрос повышения эффективности противодействия им в настоящее время как никогда актуален.

Одним из возможных способов решения проблемы может стать организация взаимодействия субъектов расследования на основе «ситуационных центров» (СЦ). Эта мера может не только повысить оперативность взаимодействия, но также обеспечить участие в расследованиях узких специалистов, снизить межведомственные барьеры.

На базе СЦ смогли бы действовать межведомственные следственно-оперативные группы с участием специалистов необходимых профилей, функционируя сменами, например, по 2–3 месяца.

[1] Оценка латентности «компьютерных» преступлений: в США – 80 %, Великобритании – 85 %, ФРГ – 75 %, России – более 90 % / Чирков Д. К., Саркисян А. Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160–181. URL: http://e-notabene.ru/nb/article_608.html.

Период привлечения специалистов может устанавливаться кратным среднему времени расследования наиболее распространенных преступлений.

В свою очередь привлекаемые специалисты смогли бы стать проводниками передового опыта для своих базовых подразделений. Очевидно, что СЦ может выполнять также функции по прогнозированию, разработке мер превентивного реагирования и профилактики, разработки нормативных правовых актов по противодействию преступности в сфере ВТ.

СЦ, построенные по территориальному принципу (на уровне одного или нескольких субъектов Федерации), могут решать следующие основные задачи:

а) расследование выявленных преступлений в сфере ВТ;

б) выявление латентных преступлений в сфере ВТ;

в) методическое обеспечение и обмен опытом расследования преступлений в сфере ВТ;

г) выработка мер профилактики (в том числе законодательных) и превентивного реагирования;

д) осуществление взаимодействия между Центрами.

Органом, уполномоченным на создание и организацию функционирования СЦ по расследованию преступлений в сфере ВТ, на наш взгляд, целесообразно определить прокуратуру России, на которую, согласно статье 1 Федерального закона «О прокуратуре Российской Федерации», возложена координация деятельности правоохранительных органов по борьбе с преступностью[1]. Дополнительным правовым основанием такого решения может стать Указ Президента России «О координации деятельности правоохранительных органов по борьбе с преступностью»[2]. Данный документ предусматривает, что «координация деятельности органов внутренних дел Российской Федерации, органов федеральной службы безопасности, войск национальной гвардии Российской Федерации, органов уголовно-исполнительной системы, таможенных органов Российской Федерации, следственных органов Следственного комитета Российской Федерации и других правоохранительных органов осуществляется в целях повышения эффективности борьбы с преступностью путем разработки и реализации

[1] О прокуратуре Российской Федерации: Федеральный закон от 17 января 1992 г. № 2202-1 (ред. от 31.12.2017) / СПС «КонсультантПлюс» (дата обращения: 30.04.2018).

[2] О координации деятельности правоохранительных органов по борьбе с преступностью: Указ Президента РФ от 18 апреля 1996 г. № 567 (ред. от 07.12.2016) / СПС «КонсультантПлюс» (дата обращения: 30.04.2018).

этими органами согласованных мер по своевременному выявлению, раскрытию, пресечению и предупреждению преступлений, устранению причин и условий, способствующих их совершению». Учитывая сопоставимый статус перечисленных правоохранительных органов, только прокуратура России имеет достаточно полномочий для эффективной организации взаимодействия в рамках СЦ по расследованию преступлений в сфере ВТ.

Таким образом, с учетом интенсивного развития и проникновения ВТ в основные сферы человеческой деятельности, совершенствование мер противодействия преступности в данной области на основе СЦ является актуальной, а возможно и безальтернативной задачей, стоящей перед правоохранительной системой Российской Федерации[1].

[1] *Долинко В.И.* Комплекс мер по обеспечению экономической безопасности тыла органов внутренних дел: Труды Академии управления МВД России. 2016. № 4 (40). С. 63–67.

Использование информационно-телекоммуникационных технологий при осуществлении незаконного оборота новых потенциально-опасных психоактивных веществ

М. М. Макаренко,
доцент кафедры,
кандидат юридических наук, доцент
(Московский университет МВД России
имени В. Я. Кикотя)

В статье рассматриваются некоторые особенности криминалистической характеристики незаконного оборота новых потенциально-опасных психоактивных веществ, а так же роль информационно-телекоммуникационных технологий при совершении указанного преступления.

Новые потенциально-опасные психоактивные вещества, криминалистическая характеристика, информационно-телекоммуникационные технологии.

Стремительно развивающаяся внешняя наркоэкспансия и насыщение наркорынка новыми видами психоактивных веществ представляют прямую угрозу национальной безопасности Российской Федерации, здоровью населения, культурному и нравственному потенциалу страны. Противодействие данной угрозе, помимо прочего, предполагает совершенствование законодательства и правоприменительной практики в указанной сфере.

Криминалистическая характеристика незаконного оборота новых потенциально опасных психоактивных веществ представляет собой систему сведений о признаках, которые являются криминалистически значимыми для данного преступления и отражают закономерные связи, возникшие между ними. Она включает в себя систему таких основных элементов, как способ, место, время и обстановка совершения преступления; типичные следы и личность преступника. Некоторые особенности этих элементов будут предметом рассмотрения в данной статье.

Понятие «дизайнерские наркотики» происходит от англ. to design (разрабатывать, проектировать). Они представляют собой психоактивные вещества синтетического происхождения, заменяющие или воспроизводящие действие наркотических средств, сходные с ними по химическому составу и вызывающие наркотическую

эйфорию. Термин «дизайнерские наркотики» появляется в 80-е гг. XX столетия и используется для обозначения синтетических опиоидных наркогенов. Такие наркотики приобретают массовую популярность в мире после появления и распространения среди несовершеннолетних преимущественно «клубных наркотиков», например МДМА (экстази)[1].

В начале XXI столетия множество аналогов наркотических средств (MDMC, 4-MMC, MMCAT и др.) становятся неотъемлемыми элементами молодежной субкультуры. Особое место в длинном перечне новых потенциально опасных психоактивных веществ занимают «курительные смеси» (CP-497, HU-210, JWH-018, JWH-250, RCS-4, RCS-8, UR-144, AB-001 и т. п.). После того как был определен основной психоактивный компонент курительных смесей, во многих странах стали приниматься антинаркотические нормы, ограничивающие или запрещающие оборот новых потенциально опасных психоактивных веществ. Такие вещества в обобщенном виде стали наименоваться «спайсами». Spice в переводе с англ. означает «специя, смесь, приправа».

Спайс и другие травяные продукты в среде обывателей называют легальными наркотиками. Они продаются чаще всего под видом лекарственных средств альтернативной медицины или как пищевые добавки. При этом большинство ингредиентов, перечисленных на упаковке, на самом деле отсутствует в продуктах спайс, а яркие психотропные эффекты возникают из-за добавления синтетических каннабиноидов, которые не указаны на этикетке. В современном научном понимании «спайс» – это любое высушенное растение, пропитанное JWH-018 (синтетический канабиойд)[2]. Наиболее распространенные продукты, продаваемые под маркой «спайс»: серебряный спайс, золотой спайс, алмазный спайс, спайс арктической синергии, спайс тропической синергии, египетский спайс и т. д. Кроме того, есть множество других растительных смесей, которым приписывается схожий эффект: «Юкатанский огонь», «Дым», «Чувство», «Удар Земли», «Лунные камни», «Голубой лотос», «Галактическое золото» и т. д. Следует отметить, что скорость инноваций в этой области настолько высока, что любой список продуктов на момент его публикации устаревает.

---

[1] *Шалагин А. Е., Усманов И. М.* Современная наркоситуация в Российской Федерации: тенденции, прогноз, меры противодействия // Вестник Казанского юридического института МВД России. 2016. № 1 (23). С. 30–34.

[2] Новости российского и мирового наркологических сообществ // Наркология. 2010. Т. 9. № 1. С. 2–11.

Наряду со «спайсом» огромной популярностью у молодежи пользуется синтетический наркотик «спиды», или «скорость», имеющий множество названий на черном рынке: СП, витамин А, озверин, порох, белый, мотиватор, фен, ботинки (или кеды, кроссы), шустрые, быстрый, амфики, антисон, рыба, кипелов, Степан Петрович и т. п. Состав «спидов» у разных производителей разный, но более 90 % «спидов» производятся из химических веществ, которые остаются при производстве героина. Таким образом, производители наркотика получают двойную выгоду, так как то, что раньше выбрасывалось, теперь отлично продается под названием «скорость». Употребляются «спиды» обычно через нос, посредством вдыхания через трубку внутрь. Иногда «спиды» употребляют при помощи колпаков (мундштуков сигарет Parliament). Реже «спиды» курят (лед). Еще реже добавляют порошок «спидов» в различные напитки, например в чай или кока-колу. Наиболее опасный и вредный способ употребления – внутривенное введение водного раствора «спидов». Такой способ используют, когда наркоман хочет достичь «спидового прихода» и сэкономить наркотик. Внутривенное употребление «спидов» позволяет наиболее экономно использовать наркотик, которого наркоману всегда не хватает[1].

Следует также обратить внимание и на то обстоятельство, что у «спайса» или синтетического канабиойда много формул. В результате чего как только правоохранительные органы запрещают одну формулу – тут же появляется другая. Токсикологическая идентификация компонентов «спайс» затруднительна, так как продукт имеет сложный химический дизайн, кроме того, в него добавляют большое количеств непсихотропных веществ, таких, например, как токоферол, которые маскируют активные компоненты. Именно по этим причинам синтетические добавки трудно обнаружить и идентифицировать[2]. По этой причине научной классификации курительных смесей в Российской Федерации не существует, так как своевременно систематизировать столь быстро пополняющийся ассортимент продукта, появившегося на отечественном рынке, специалисты не успевают.

В Россию большая часть такого рода веществ поступает из Китая. Средний вес одного изъятия, поступившего из КНР,

---

[1] *Каклюгин Н.В.* Синтетическая Россия: прогрессирующее самоубийство наркотизирующейся молодежи: Проблемы и перспективы // Медицина. 2014. Т. 2. № 4 (8). С. 1–27.

[2] *Курдиль Н.В.* Актуальные вопросы таксикологии и лабораторной идентификации синтетических каннабиноидов (подготовлено по материалам Европейского Центра наркотиков и наркомании EMCDDA) // Медицина неотложных состояний. 2015. № 2 (65). С. 9–18.

составляет 480 граммов, из других государств – 16 граммов[1]. Мониторинг сети Интернет показывает, что в КНР имеется значительное число предприятий химической промышленности, производящих новые виды психоактивных веществ. Например: «Nanjing Hong Xiang Chemical Industry Co. Ltd.», «LongPan road No.173 Nanjing Jiangsu 210007 China». Эти компании производят синтетические каннабиноиды JWH-122, JWH-250, JWH-019, JWH-081, JWH-203, JWH-210, JWH-251. «Jwhchemical, co., ltd, Room 101, block 5, No 1621 Nanmatou road, Shanghai, China 200210» – производит и предлагает к продаже на своем сайте JWH-018, JWH-073, JWH-200, JWH-250, JWH-019, JWH-210, JWH-122, JWH – 081.

К продаже предлагаются партии от 5 до 100 грамм, по предварительному заказу возможна поставка партий от 250 грамм до 100 кг. Цена от 10–20 долл. за грамм (100 г) до 27–54 долл. за грамм (5 г) – в зависимости от вида психоактивного вещества.

Доставка осуществляется международными курьерскими службами: EMS, FedEx, UPS, TNT. Оплата производится с использованием платежных систем Alipay.com, PayPal, Western Union, Alert Pay.

Распространение данных видов наркотиков осуществляется двумя основными способами. Первый способ наиболее простой, когда наркотики распространяют в ночных клубах в основном молодым, чаще даже не достигшем 18-летнего возраста девушкам, у которых употребление «спидов» вызывает непреодолимое половое влечение. Именно за это свойство «скорость» пользуется огромной популярностью у молодых людей, которые «угощают» наркотиками девушек в ночных клубах.

Другой способ распространения данных веществ бесконтактный, так называемая «закладка». Этот способ основан на использовании информационно-телекоммуникационных технологий. Второе десятилетие XXI в. характеризуется тем, что для сбыта искомых объектов, оперативного обмена необходимой информацией (характер товара, места закладок), в том числе визуальной, с 2011–2012 гг. преступники активно используют возможности сети Интернет, в частности такие ресурсы, как Skype, Brosix, Jabber, ICQ и др. Используя такой способ, «покупатель» заказывает определенное количество наркотика, после чего переводит необходимую сумму электронных денег на электронный счет «продавца». При этом, как правило, используются системы «Вебмани» и «Скрил». После

[1] *Сухаренко А.* Расплата за спайс // ЭЖ-Юрист. 2015. № 7. С. 2.

поступления денег на счет «продавец» отправляет «покупателю» сведения о конкретном адресе и месте, где находится наркотик. После чего наркоман приходит в указанное место и забирает его.

В реализации этой преступной схемы участвует, как правило, хорошо организованная структурированная группа преступников, каждый из которых наделен своей функцией. Основу данной группы составляет, так называемый «закладчик». Это, как правило, участник соответствующего интернет-форума, который за каждую «закладку» получает вознаграждение до 200 руб. и больше. Закладчики подразделяются на простых и оптовых. Последние получают адреса закладок от оператора, а их гонорар составляет определенный процент от суммы, вырученной от продажи новых опасных психоактивных веществ.

Оператор выступает в качестве связующего звена между базами, где производится закладка, закладчиками и потребителями. Он изучает конъюктуру и потребности преступного рынка, осуществляет деятельность по рекламе предлагаемого продукта на соответствующих интернет-форумах и в чатах.

Следующая немаловажная фигура – это финансовый менеджер, занимающийся обобщением отчетов о продажах, оформлением Qiwi-кошельков, контролем движения по электронным счетам, куда поступают деньги за предлагаемый товар.

Важное доказательственное значение имеют и показания хакера, являющегося консультантом по всем техническим вопросам. Условно его можно назвать своего рода специалистом по «информационной безопасности». Именно в его обязанности входит создание условий для безопасного использования информационно-телекоммуникационных технологий в незаконном обороте новых наиболее опасных психоактивных веществ, в том числе посредством использования «Brosix», «Skype» и «ICQ». В числе прочего он выдает логины и пароли для указанных программ через интернет-сервис безопасного обмена данными http://privnote.com.

Среди остальных участников группы можно назвать курьеров, осуществляющих транспортировку крупных партий запрещенного продукта (от 1 кг. и выше), кладовщиков, занимающихся хранением этих крупных поставок, а также координаторов, контролирующих все звенья преступной схемы.

Как правило, основными участниками незаконных операций по продаже наркотических средств, психотропных и новых потенциально опасных психоактивных веществ являются молодые люди

в возрасте от 17 до 29 лет, нередко учащиеся (студенты), лица, не имеющие постоянного места работы (источника дохода).

В заключение следует отметить, что разработка преступных групп, осуществляющих сбыт наркотиков через сеть Интернет и систему электронных платежей, достаточно сложна, требует детального и длительного документирования фактов преступной деятельности, значительного количества привлекаемых сил и оперативно-технических средств. Рассмотренные же в рамках данной статьи особенности некоторых элементов криминалистической характеристики незаконного оборота новых потенциально-опасных психоактивных веществ будут способствовать надлежащему построению и проверке следственных версий при осуществлении расследования по уголовным делам, возбужденным по фактам совершения данного преступления.

Проблемы противодействия взяточничеству, совершаемого с использованием информационно-телекоммуникационных технологий

А. П. Макаров
(Прокуратура Нахимовского района г. Севастополя)

В статье рассматриваются проблемные вопросы противодействия взяточничеству на современном этапе развития информационно-телекоммуникационных технологий. При этом основное внимание уделено аспектам противодействия фактов этого опасного явления, совершенного путем использования платежных систем.

Коррупционные преступления, взяточничество, платежные системы, информационно-телекоммуникационные технологии, электронные платежи, электронный кошелек.

Взяточничество как элемент коррупции является прямой угрозой стабильного функционирования государственных органов, осуществления правосудия; противоречит одному из основных принципов современного развитого общества – принципу равенства.

Взяточничество имеет далекие исторические корни и считается одним из самых опасных для общества пороков. При этом искоренение коррупции на протяжении всей истории человечества велось во всех странах мира с переменным успехом. Окончательно искоренить взяточничество и коррупцию еще никому не удавалось. С этапом глубокой информатизации общества, а также развития новых технологий возникли новые способы совершения коррупционных преступлений.

При подведении итогов работы Генпрокуратуры за 2017 г. ведомство оценило число выявленных коррупционных преступлений за прошлый год в 29,6 тыс. Удельная доля дел о взяточничестве в общем числе возбужденных дел составила 1,4 %. За указанный период число осужденных за взяточничество 36 % составили государственные служащие, 30 % – сотрудники МВД, 12 % – руководители коммерческих структур, 2 % – сотрудники следственных органов и прокуратуры[1].

[1] Генпрокуратура подсчитала осужденных за взятки силовиков [Электронный ресурс]. URL::ttps://www.rbc.ru/society/23/04/2018/5add8b6a9a794753f141c37c?utm_source=gismeteo&utm_medium=news&utm_campaign=gism_top2. Загл. с экрана (дата обращения: 17.04.2018).

До момента существования банковской системы и системы денежных переводов единственным способом дачи взятки являлась непосредственная передача одного лица или через посредника другому денежных средств либо иных материальных благ.

С целью выявления и фиксации фактов взяточничества оперативными подразделениями в порядке, установленным законодательством,[1] осуществляется документирование преступных действий подозреваемых лиц. А как же обстоит дело с выявлением скрытых фактов взяточничества, таких как получение и передача взятки путем перевода денежных средств на банковские счета, электронные кошельки и сервисы?

В настоящее время преступники используют электронные платежи в банковских компьютерных сетях (Свифт, Спринт-Теленет, EPS-Net, SMS и др.). С их помощью покупаются акции, валюта, государственные казначейские обязательства и другие ценные бумаги, используются международные электронные платежи в сети Интернет (электронные кошельки, цифровые и сетевые бумажники) системы Cybercash, DigiCash и NetCash и др.[2]

Существуют популярные платежные системы и системы денежных переводов, такие как Юнистрим, Лидер, Яндекс.Деньги, Blizko, Contact, PayPal, Swift, WebMoney. При этом данный перечень не является исчерпывающим и имеет тенденцию пополняться новыми системами и организациями в сфере финансовых телекоммуникаций. Современные сервисы предлагают возможность перечисления денежных средств как с персонифицированных аккаунтов, так и с зашифрованных или обезличенных источников. В некоторых случаях правоохранители, зная о перечислении денежных средств должностному лицу, сталкиваются с проблемой идентификации взяткодателя, анонимно перечислившего денежные средства в пользу взяточника. К примеру, злоумышленник может с помощью обычных уличных терминалов пополнить электронный кошелек взяткополучателя в сервисе Яндекс денежными средствами на сумму до 15 000 руб. без раскрытия своих персональных данных.[3] Ана-

---

[1] Об оперативно-розыскной деятельности: Федеральный закон № 144-ФЗ от 12 августа1995 г. (ред. от 06.07.2016) [Электронный ресурс]. URL: http: // www. co№sulta№t.ru (дата обращения: 19.04.2018).

[2] *Тлиш А.Д.* Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт: дис. ... канд. юрид. наук: Краснодар, 2002. 253 с.

[3] Пополнение кошелька [Электронный ресурс]. URL:https://yandex.ru/support/money/add/to-wallet.html (дата обращения: 05.04.2018).

логичного рода пополнения и переводы возможны с помощью иных коммуникационных систем.

Естественно, что при наличии на то правовых оснований владельцы сервисов в предусмотренном законом порядке предоставляют суду и правоохранителям имеющиеся сведения о проведенных операциях. Но это происходит только в том случае, если об этих операциях сомнительного происхождения стало кому-нибудь известно. Данное взаимодействие в основном реализовывается в рамках расследования интернет-мошенничеств.

Таким образом, в случае если правоохранительным органам заранее не известно о сговоре взяткодателя и взяткополучателя, договорившихся о способе передачи денежных средств, то установить и задокументировать данный факт будет весьма сложно.

Так, совместная работа ФСБ и Генеральной прокуратуры РФ позволила предотвратить ряд коррупционных преступлений и нанесения значительного ущерба экономике страны при готовящейся приватизации управляющей компании АО «Роснано». В результате информирования Президента Российской Федерации органами ФСБ России приостановлен процесс приватизации и не допущено утраты государственного контроля над активами портфельных компаний АО «Роснано» на сумму 147 млрд рублей[1].

С целью противодействия взяточничеству, совершенного при помощи платежных систем, И.М. Сперанским предложено внести дополнения в постановление Пленума Верховного Суда РФ от 09.07.2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» для уточнения способа передачи и получения взятки, а именно дистанционно через платежные системы[2].

Как правило, успех в расследовании взяточничества с использованием информационно-коммуникационных технологий зависит не только от быстрого начала предварительного расследования в отношении лиц, совершивших уголовно наказуемое деяние, но и от умения следователя использовать все силы и средства для раскрытия преступления, оперативные возможности подразделений правоохранительных органов и экспертных учреждений.

Хотелось бы подчеркнуть, что проведение экспертиз по данной категории дел и полученные доказательства в ходе их проведения

---

[1] Приватизация УК «Роснано» была остановлена Путиным после сигнала ФСБ. URL: http://www.interfax.ru/russia/608954?utm_referrer=https%3A%2F%2Fzen.yandex.com (дата обращения: 20.04.2018).

[2] *Сперанский И.М.* Проблемные вопросы, связанные с расследованием получения и дачи взятки при помощи платежных систем // Интеграция наук. 2017. № 1 (5). С. 47–49.

могут стать основными и (или) единственными доказательствами по уголовному делу.

В ходе раскрытия и расследования взяточничества, совершаемого с использованием НИТ, на должном уровне еще не отработаны тактические и методические аспекты организации проведения расследования, а также особенности проведения отдельных следственных действий, таких как производство следственного осмотра, обыска, выемки и фиксации следов преступной деятельности взяточников.

При этом необходимо подчеркнуть на необходимость обладания специальными познаниями следователем и лицами, принимающим непосредственное участие в раскрытии и расследовании данной категории дел.

Использование информационно-коммуникационных технологий не только позволяет бороться с коррупционными проявлениями при использовании информационной открытости органов государственной и исполнительной власти, но и дает возможность преступникам скрыть свои противоправные деяния, используя несовершенство действующего уголовного и уголовно-процессуального законодательства, анонимность сети Интернет, отсутствие необходимых современных национальных стандартов и технологий по противодействию коррупции и др.

Среди ученых-юристов уже длительное время рассматривается вопрос о возможности и целесообразности установления уголовной ответственности за совершение коррупционных преступлений со стороны юридических лиц, которые совершаются в интересах или от имени юридических лиц[1].

Конечно, согласно классическому подходу к понятию преступления многими учеными уголовная ответственность юридических лиц воспринимается как нечто неприемлемое. Однако, учитывая активное и наступательное противодействие коррупционным проявлениям, взяточничеству со стороны государства и общества, введение данной уголовной нормы в действующее законодательство представляется не только необходимым, но и возможным в ближайшем будущем.

В связи с этим можно сделать вывод, что преступники, совершающие коррупционные деяния, в том числе и взяточничество, постоянно совершенствуют способы совершения преступления с помощью компьютерных информационных технологий, приспо-

[1] *Цирин А. М., Черепанова Е. В., Тулинова О.А.* Современные стандарты и технологии противодействия коррупции // Журнал российского права. 2014. № 7. С. 143–171.

сабливаются к действующему законодательству, постоянно меняют свою тактику и варианты решения для достижения конечной преступной цели – получение коррупционных доходов.

Внедрение информационно-телекоммуникационных технологий в борьбе с коррупцией как на региональном, так и на федеральном уровне сталкивается с рядом проблем, среди которых: создание новых антикоррупционных стандартов, обеспечение правовой поддержки, необходимость использования соответствующих технологий и оперативного обеспечения, проведение тщательного расследования и санкций, представление доказательств.

Поэтому государство должно постоянно взаимодействовать с наиболее активными представителями гражданского общества в борьбе со взяточничеством, объединить усилия неправительственных организаций и бизнеса в борьбе с коррупционными правонарушениями, совершенствовать антикоррупционную деятельность органов государственной власти и органов местного самоуправления.

О некоторых проблемах допустимости доказательств в уголовном процессе при изъятии компьютерной информации с мобильных устройств связи

О. В. Макарова,
ведущий научный сотрудник,
кандидат юридических наук
(Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации)

В статье анализируется ряд проблем, связанных с допустимостью доказательств в уголовном процессе при изъятии компьютерной информации с мобильных устройств связи. Отмечается, что компьютерная информация может служить как орудием преступления либо предметом преступления, так и информацией о следах преступления, зафиксированных с помощью протоколирования и аудита информационной системы.

Мобильное устройство связи, компьютерная информация, следственные действия, оперативно-разыскные мероприятия.

В современном мире мало найдется людей, которые не используют мобильные системы связи (сотовые телефоны, смартфоны, планшеты, компьютеры устройства GPS и др.). Все они содержат персональные данные, сохраняют множество операций с электронной информацией, включая историю банковских операций, историю соединений с абонентами, переписку в социальных сетях и электронной почте, фотографии и видео, личные записи и заметки. При этом мобильные системы связи не только содержат и сохраняют разную информацию, но и обладают возможностью ее извлечения.

Федеральным законом от 28.07.2012 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» ст.ст. 81, 82, 166, 182, 183 УПК РФ дополнены таким источником доказательств, как «электронный носитель информации». Регламентированы основания и порядок производства обыска и выемки электронных носителей информации, изъятие и копирование которых должно производиться при обязательном участии специалиста.

Вместе с тем остаются нерешенными ряд проблем, связанных с допустимостью такого рода доказательств. К примеру, следователю при изъятии в ходе осмотра места происшествия предоставля-

ется доступ к компьютерной информации мобильного устройства связи без императивного указания на наличие судебного решения, что, по сути, создает предпосылки для обжалования этих действий как необоснованное нарушение конституционных прав и свобод человека. В результате создаются реальные возможности признания судом таких действий незаконными.

Под вещественными доказательствами в уголовно-процессуальном праве понимаются предметы, вещи, в том числе документы. А содержанием вещественного доказательства являются следы, свойства, признаки, которые непосредственно зафиксированы на предмете, доступны непосредственному восприятию и могут быть обнаружены путем осмотра. Таким образом, основным признаком вещественного доказательства является его объективная связь с предметом доказывания, в силу которой оно и может служить средством установления доказываемых фактов. Указанный признак в полной мере можно отнести к компьютерной информации, которая может служить как орудием преступления либо предметом преступления, так и информацией о следах преступления, зафиксированной с помощью систем протоколирования и аудита информационной системы.

Следственный осмотр является одним из самых распространенных следственных действий. Процессуальный порядок осмотра предусмотрен ст.ст. 176–180 УПК РФ. Суть осмотра заключается в непосредственном определении следователем наличия фактов, имеющих доказательственное значение. В случае формирования электронного доказательства в сфере компьютерной информации главными условиями выступают процессуальная форма и правовой статус субъекта, уполномоченного оценивать эту информацию как факт.

Поскольку осмотр мобильных устройств отличается от иных видов осмотра тем, что компьютерная информация, содержащаяся в мобильном устройстве связи, зачастую не может восприниматься человеком непосредственно органами чувств, воспринимать (следовательно и осмотреть в смысле УПК РФ) ее можно с помощью технических и программных средств. Таким образом, осмотр мобильных устройств связи, в частности и любой компьютерной информации в целом, это не столько осмотр как таковой, а скорее техническое исследование, требующее определенных знаний[1].

[1] См. подробнее: *Вехов В.Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография // Волгоград: ВА МВД России, 2008.

Следует отметить, что речь идет о двух самостоятельных действиях, первое из которых – изъятие мобильного устройства связи и второе – извлечение информации из памяти мобильного устройства связи или SIM-карт, карт памяти.

Получить мобильное устройство связи можно при:

– осмотре места происшествия (ст. 176 УПК РФ);

– осмотре трупа (ст. 178 УПК РФ);

– обыске (ст. 182 УПК РФ);

– выемке (ст. 183 УПК РФ);

– личном обыске подозреваемого/обвиняемого (ст.ст. 93, 184 УПК РФ).

При этом выемку мобильного устройства могут осуществить также сотрудники органа дознания по письменному поручению следователя, в производстве которого находится уголовное дело, но обязательно с участием специалиста.

Оптимальным вариантом осмотра мобильного устройства связи, как носителя информации, является фиксация конфигурации на месте обнаружения, а также история посещенных сетевых ресурсов, история программ обмена короткими сообщениями, фото-, аудио – и видеоинформация, удаленные данные, геолокационные данные и другая криминалистически значимая информация. К примеру, в настоящее время для получения компьютерной информации с мобильных устройств связи правоохранительными органами широко используется устройство криминалистического исследования «UFED»[1], обеспечивающее быстрое и безопасное извлечение важнейших криминалистических данных из мобильных телефонов, смартфонов, навигаторов и др.

К таким данным относятся:

– телефонная книга, текстовые сообщения, фотографии, видеоизображения, журналы звонков (исходящих, входящих, пропущенных), звуковые файлы, ESN, IMEI, ICCID и IMSI;

– удаленные, скрытые файлы, пароли;

– доступ к заблокированным данным путем обхода, открытия или отключения пользовательского кода блокировки;

– дешифрованные данные журнала поэтапной регистрации и извлечение данных из других переносных устройств GPS;

– дешифрованные данные базы данных истории различных мессенджеров.

---

[1] Криминалистическое оборудование. Системы экспертизы. Средства экспертизы электронных устройств. Средства исследования мобильных телефонов и смартфонов // URL:http://www.bnti.ru.

Федеральным законом 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» в Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) внесено изменение, согласно которому перечень оперативно-разыскных мероприятий был расширен новым видом – «получение компьютерной информации» (п. 15 ч. 1 ст. 6). Следует отметить, что до внесения указанных изменений все действия с компьютерной информацией проводились в рамках оперативно-разыскного мероприятия: «снятие информации с технических каналов связи» (ст. 8 Закона об ОРД).

По справедливому замечанию А.Л. Осипенко, в техническом плане «получение компьютерной информации» может осуществляться, в том числе, и при непосредственном доступе к устройствам памяти, установленным в компьютере и периферийном оборудовании. При этом цитируемый автор получение информации с технических каналов связи с объектов, полученных гласным путем, рекомендует оформлять «через иные оперативно-разыскные мероприятия (наведение справок, сбор образцов для сравнительного исследования, проводимое гласно обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.)»[1].

Отсутствие наработанной практики проведения такого вида оперативно-разыскного мероприятия, как «получение компьютерной информации», а также наличие высокого риска, связанного с ограничением конституционных прав человека на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, усложняет его активное применение и реализацию его потенциала при решении задач оперативно-разыскной деятельности.

Анализ правоприменительной практики свидетельствует еще об одной проблеме, способной привести к признанию доказательств недопустимыми. Речь идет об отсутствии ясной законодательной регламентации действий, направленных на корректное изъятие компьютерной информации с мобильных устройств связи, обеспечивающих защиту конституционных прав и свобод граждан, а также достижения задач оперативно-разыскной деятельности. На прак-

[1] *Осипенко А.Л.* Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 83–90.

тике компьютерную информацию изымают, включая электронные сообщения, по основаниям, предусмотренным п. 5 ч. 2 ст. 7 Закона об ОРД без судебного решения, получая согласие лица в письменной форме или оформляя результатами проведенного оперативно-разыскного мероприятия «исследование предметов и документов». При таком положении дел высока потенциальная вероятность признания доказательств недопустимыми. В соответствии с ч. 1 ст. 75 УПК РФ доказательства, полученные с нарушением требований УПК, являются недопустимыми, а согласно ст. 89 УПК РФ запрещается использование результатов оперативно-разыскной деятельности, если они не отвечают требованиям, предъявляемым к уголовно-процессуальным доказательствам.

Таким образом, возможность быстрого раскрытия преступлений по горячим следам, получение необходимой информации для подтверждения или опровержения предварительных подозрений в совершении преступлений требует от законодателя дополнительного правового регулирования, позволяющего правильно оформлять результаты изъятой компьютерной информации и в дальнейшем использовать в качестве доказательств при расследовании преступлений, без нарушения конституционных прав граждан.

Документирование результатов оперативно-разыскной деятельности и их использование как повода и основания для возбуждения уголовного дела о незаконном сбыте наркотических средств бесконтактным способом с использованием информационно-телекоммуникационных сетей

Н. В. Макеева,
кандидат юридических наук,
доцент
(Московский университет МВД России
им. В.Я. Кикотя)

В статье рассматривается деятельность следственных органов и оперативных подразделений при решении вопроса о возбуждении уголовного дела о незаконном сбыте наркотических средств бесконтактным способом с использованием информационно-телекоммуникационных сетей.

Сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием информационно-телекоммуникационных сетей (включая сеть Интернет), поводы и основание для возбуждения уголовного дела, результаты ОРД.

В соответствии со ст. 228.1 УК РФ установлена уголовная ответственность за сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием информационно-телекоммуникационных сетей (включая сеть Интернет). Такой способ сбыта на практике и в юридической литературе принято называть «бесконтактным способом сбыта наркотических средств». Это под собой подразумевает сбыт наркотиков новым способом, когда сбытчик и незаконный приобретатель не встречаются лично, а договариваются о приобретении наркотических средств, оплачивают их получение, получают сведения о местонахождении тайника с использованием мобильной связи или сети Интернет. Появляющиеся новые способы сбыта заставляют сотрудников органов внутренних дел менять способы фиксации сбыта, в том числе с использованием материалов оперативно-разыскной деятельности.

Статья 140 УПК РФ рассматривает в качестве одного из поводов для возбуждения уголовного дела сообщение о совершенном или готовящемся преступлении, полученное из иных источников.

Одним из источников таких сведений и являются результаты оперативно-розыскной деятельности. Однако не следует забывать о том, что в чистом виде полученные результаты ОРД не являются поводом для возбуждения уголовного дела, таковым является лишь рапорт, представленный оперативным подразделением по результатам производства ОРМ. Основанием же для возбуждения уголовного дела в рамках указанного повода служат материалы, полученные в ходе осуществления оперативно-розыскных мероприятий.

Располагая информацией, предоставленной оперативным подразделением, следователь производит юридическую оценку с целью проверки оснований для возбуждения уголовного дела и тем самым ее трансформацию в дальнейшем в доказательства.

Для решения вопроса о возбуждении уголовного дела следователь должен дать юридическую оценку полученным материалам ОРМ, а именно:

– рассмотреть их со стороны достаточности для принятия процессуального решения;

– в представленных материалах должны иметь место данные, указывающие на признаки преступления (если полученных данных не будет достаточно для принятия решения о возбуждении уголовного дела, следователь возвращает их через начальника ОМВД с письменным изложением обстоятельств, препятствующих его возбуждению, и мероприятий, подлежащих выполнению для устранения имеющихся пробелов).

Чаще всего при поступлении информации о факте совершения противоправных действий, связанных с незаконным оборотом наркотических средств или психотропных веществ, осуществляются такие оперативно-разыскные мероприятия, как: проверочная закупка; наблюдение; оперативный эксперимент; обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров.

Особенностью бесконтактного способа сбыта является то, что сбыт чаще всего осуществляется организованной группой, в которой все роли четко распределены. В структуру группы входят: «организатор», «оператор», «закладчик», «вербовщик», «кладовщик», «системный администратор», «экспедитор»[1]. Вступая меж-

[1] *Помелов А.А.* Некоторые вопросы документирования сбыта наркотических средств с использованием сети Интернет // XXI Международная научно-практическая конференция «Деятельность правоохранительных органов в современных условиях». Иркутск, 2016. С. 78–81.

ду собой в преступный сговор, эти лица действуют с использованием удаленного сервера, электронных и информационно-телекоммуникационных сетей, размещают информацию о виде, весе, цене предлагаемого наркотика, а также способах связи и оплате на сайтах в сети Интернет. При этом после поступления денежных средств на электронные платежные системы (QIWI-банк; ЯндексДеньги; WebMoney) осуществляют передачу наркотических средств через систему тайников, место расположение которых сообщают после оплаты с помощью средств мобильной связи. Такой способ сбыта характеризуется тем, что нижестоящие участники не знают вышестоящих. Это осложняет процесс их выявления и доказывания незаконной деятельности организованной группы.

В связи с этим органами внутренних дел отрабатываются алгоритмы деятельности, в том числе связанные с фиксацией факта сбыта бесконтактным способом на этапе возбуждения уголовного дела. Особенностью деятельности на этом этапе является: длительное документирование факта преступной деятельности, привлечение значительного числа технических средств и специалистов оперативно-технических подразделений, координация действий с высококвалифицированными следователями.

Чаще всего при поступлении информации о факте совершения противоправных действий, связанных с незаконным оборотом наркотических средств или психотропных веществ, осуществляется проверочная закупка. Соблюдение законности в рамках проведения и фиксации результатов проверочной закупки позволит в дальнейшем использовать материалы ОРМ при решении вопроса о возбуждении уголовного дела, что подтверждается следующим алгоритмом действий лиц, участвующих в ее проведении:

1) проведение проверочной закупки наркотических средств или психотропных веществ возможно лишь на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-разыскную деятельность (ч. 7 ст. 8 ФЗ об ОРД), которое является основанием для начала ее проведения;

2) перед проверочной закупкой «покупатель» обязательно досматривается в присутствии понятых на предмет отсутствия у него наркотических средств, что фиксируется в протоколе досмотра. В качестве покупателя могут участвовать лица, решившие на добровольной основе сотрудничать с оперативными подразделениями, а также оперативные сотрудники (их досмотр не производится). Весь ход проверочной закупки фиксируется с помощью аудио – или видеосредств фиксации;

3) по результатам проверочной закупки составляется протокол добровольной выдачи наркотических средств лицом, участвовавшем в качестве покупателя. Также составляется протокол выдачи технических средств в том случае, если они ему выдавались;

4) при задержании лица, осуществлявшего закладку наркотических средств, в рамках производства проверочной закупки составляется протокол личного досмотра в соответствии с требованиями КоАП РФ (ст.ст. 27.1, 27.7, 27.9, 27.10) и принимаются меры, предупреждающие возможное сокрытие или уничтожение наркотических средств, электронных носителей информации (SIM-карты, флэш-карты и т. д.);

5) у задержанного лица, участвовавшего в качестве «покупателя», у понятых (представителей общественности) берутся объяснения. У «покупателя» выясняется:

– где, когда и при каких обстоятельствах производилась проверочная закупка;

– каким образом он связывался с продавцом (указывает все имеющиеся у него о нем сведения: абонентские номера телефонов,в т.ч. в котором используются Viber, WhatsAppMessenger, номер ICQ, ник в Skype, Brosix, Jabber);

– где обнаружил тайник с наркотическими средствами или где происходила их передача;

– какое количество наркотических средств было приобретено и по какой цене;

– каким образом осуществлялась оплата (через какие системы оплаты).

У задержанного, осуществлявшего закладку наркотических средств, выясняется:

– принадлежность изъятых наркотиков;

– кто еще участвовал в сбыте наркотиков;

– где осуществлялось приобретение, изготовление, перепродажа наркотических средств, в каком количестве, когда и по какой цене.

– кто поставщик наркотиков;

– каким образом осуществлялась доставка наркотических средств;

– кто вручал НС, присутствовал ли кто-нибудь при этом;

– в каком количестве и какой упаковке были получены наркотики;

– где осуществлялась расфасовка;

– кому реализовывались наркотические средства, каким способом т. д.;

6) изъятые наркотические средстве направляются на судебную экспертизу (или предварительное исследования), в ходе

которой устанавливается, является ли изъятое вещество наркотическим, его вид и объем;

7) при привлечении специалистов оперативно-технических подразделений ими устанавливаются: процесс общения покупателя с оператором посредством средств сотовой связи или Интернета, как осуществлялась«оплата» за приобретаемое наркотическое средство через терминал самообслуживания (мультикассу)[1]. При использовании технических средств фиксации с видеоносителей может быть получена информация о непосредственном приобретении наркотических средств в тайнике;

8) собранные в ходе проведения проверочной закупки материалы вместе с рапортом об обнаружении признаков преступления передаются начальником оперативно-розыскного подразделения, проводившего разработку, руководителю следственного органа.

В перечень документов, предоставляемых оперативно-разыскными подразделениями органам предварительного следствия, как правило, входят:

– постановление о предоставлении результатов ОРД, с перечнем документов, подлежащих направлению;

– постановление о рассекречивании сведений, составляющих государственную тайну и их носителей, подписанное начальником соответствующего территориального органа;

– постановление о проведении ОРМ, подписанное начальником оперативно-разыскного подразделения и утвержденное начальником территориального органа;

– согласие лица о добровольном оказании содействия;

– протокол досмотра вещей, принадлежащих участнику проверочной закупки, при необходимости – его автомобиля;

– протоколы вручения денежных средств, предметов, ценностей;

– протоколы вручения технических средств видео – и звукозаписи;

– протокол добровольной выдачи приобретенных средств и веществ;

– протоколы выдачи технических средств;

– заключение эксперта или справки специалиста о принадлежности выданных веществ к наркотикам;

– объяснения понятых (представителей общественности), «покупателя», очевидцев преступной деятельности и лица, осуществлявшего закладку наркотических средств;

---

[1] *Шебалин А.В.* Расследование незаконных сбытов наркотических средств, совершенных бесконтактным способом: учебное пособие. Барнаул, 2015. С. 12–13.

– акт проведения ОРМ(к акту прилагается фототаблица со скриншотами или фотографиями экранов компьютеров, смартфонов, телефонов, на которых изображена переписка с оператором, фотографии с мест нахождения закладок)[1];

– рапорта сотрудников оперативных подразделений о ходе и результатах проведенных ОРМ;

– рапорт об обнаружении признаков преступления.

Получив вышеперечисленные документы, следователь осуществляет проверку результатов оперативно-разыскной деятельности на предмет их соответствия требованиям закона, после чего принимает меры к приданию им доказательственного значения. Результаты ОРМ в дальнейшем, в случае их законного происхождения, служат поводом и основанием для возбуждения уголовного дела и используются в доказывании по уголовным делам. Если в материалах проверки есть сведения, указывающие на использование информационно-телекоммуникационных сетей, то следователь должен квалифицировать действия по п. «б» ч. 2 ст. 228.1 УК РФ. Несмотря на существующие явные проблемы, связанные со сложным процессом выявления и фиксирования преступлений, совершенных бесконтактным способом, на сегодняшний день такого рода преступления успешно выявляются оперативными подразделениями и расследуются органами предварительного следствия.

[1] *Там же*. С. 12.

Развитие метода компьютерного моделирования места происшествия и других объектов криминалистического исследования

С. В. Маравина,
студентка
(ННГУ им. Лобачевского)

В статье рассматривается проблематика использования и развития компьютерного моделирования при осмотре места происшествия, изучении улик, получения доказательственной информации и обучения специалистов.

Компьютерное моделирование, виртуальный осмотр места происшествия, 3D-модель, специалист-криминалист.

Проблема развития компьютеризации всех сторон жизни человечества является одной из наиболее актуальных XXI в. Однако существуют конкретные направления, на которые современной наукой делается особый акцент, так как они способствуют нормальному функционированию и безопасности жизни государства в целом[1]. Одним из таких направлений является криминалистическая техника, развитие которой способствует наиболее эффективному и быстрому раскрытию различного рода преступлений.

Наиболее прогрессирующим направлением развития криминалистической техники является компьютерное моделирование, которое в будущем, во-первых, обеспечит эффективное обучение молодых следователей, воссоздавая виртуальную обстановку места происшествия, позволяя при этом экономить средства на различных муляжах и полигонах, и, во-вторых, постепенно может заменить систему криминалистической фотографии 3D-моделью места происшествия.

Российскими учеными также ведутся и даже уже используются разработки в данном направлении. Так, специалистами в области компьютерных технологий была создана программа «Виртуальный осмотр места происшествия», которая переросла в целый программный комплекс Управления криминалистики Следственного комитета Российской Федерации. Основатели стартапа FSA 3D

[1] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

Investigation (ООО «Фундаментальные системы анализа») Фархад Ашимов и Антон Козлов из Астрахани.

FSA 3D Investigation уже поставила учебные симуляторы обоих типов во все региональные подразделение Следственного комитета – их более сотни, в каждом оснащены от 1–2 до 10–15 автоматизированных рабочих мест. Программное обеспечение приобретают и подразделения МВД России, и Генпрокуратуры РФ, а также более 35 вузов, включая МГУ им. М.В. Ломоносова и Московский университет МВД России[1].

Особенно активно в данный момент программный комплекс используется в учебном кабинете криминалистики Следственного комитета РФ по Республике Татарстан для лиц, впервые назначенных на должность следователей, и для следователей, проходящих повышение квалификации.

В настоящий момент программа носит лишь обучающий характер и представляет собой тренажер-симулятор, создающий интерактивные 3D сцены, имитирующие различные уникальные места преступлений, что позволяет заменить учебные полигоны с различными муляжами и воссозданной остановкой. Данные интерактивные 3D сцены позволяют исследовать территорию и объекты в режиме реального времени, перемещаться в пространстве и рассматривать любые ракурсы, а заложенные в программу библиотеки из 500 готовых объектов и 50 инструментов для обнаружения, изъятия и упаковки улик позволяют не просто присутствовать в виртуальном пространстве, а участвовать, действовать, получать и совершенствовать навыки работы с криминалистической техникой и инструментами, выдвигать гипотезы и разрабатывать версии.

Тренажер «Виртуальный осмотр места происшествия» работает следующим образом: преподаватель создает 3D-модель места преступления, он может выбрать тип квартиры определенной планировки, разместить в ней мебель, определить местоположение и позу трупа, разбрызгать кровь и разбросать предметы, которые могут служить уликами. Каждый из объектов и следов может находиться в любой плоскости, например капли крови можно оставить не только на полу, но и на стене, а пистолет может оказаться не только на поверхности стола, но и под диваном. Можно устроить беспорядок, разбросав вещи по полу, спрятав в них улики – вроде забытой преступником перчатки или гильзы. Также к предметам

[1] *Скобелин С. Ю., Кузнецов В.В.* Инновационный способ фиксации осмотра места происшествия с использованием высоких технологий // Российский следователь. 2018. № 1. С. 35–38.

можно добавить подсказки – например указание на главу из учебника, а комментарии могут содержать не только текстовую, но и аудио – и видеоинформацию. Чтобы собрать улики, обучающиеся пользуются приложенными инструментами: виртуальными дактилоскопическими кистями, тампонами для сбора крови и гипсом для снятия отпечатков обуви. Для наглядности и закрепления практических навыков различные сцены можно проиграть в классе – продемонстрировать аудитории, как правильно провести осмотр или оставить учеников с заданием один на один, чтобы у них была возможность разобраться с поставленными задачами самостоятельно, но под руководством преподавателей.

Другой тренажер от FSA 3D Investigation позволяет проводить виртуальные обыски. Принцип его действия тот же, однако имеются специальные инструменты осмотра: например, при выборе металлодетектора возможно осуществление поиска тайников, а георадар способствует обнаружению зарытых предметов или скрытых полостей, где может быть взрывчатка или наркотики.

В двух этих программах – 12 локаций и более 20 сцен (например, в локации «вокзал» могут быть сцены: «вокзал», «подземный переход», «ж/д пути»), более пятисот объектов в девяти категориях.

Высокую степень реалистичности виртуального пространства позволяет создать шлем виртуальной реальности типа Oculus Rift и аналогичные ему технические приспособления, которые обеспечивают несравнимое ощущение погруженности и включенности в процесс благодаря 3D-изображению и углу обзора в 110°, стереозвуку и интуитивному Touch-управлению, которое позволяет взаимодействовать с виртуальной реальностью так же естественно, как с реальным миром.

Для наиболее эффективного и прогрессивного обучения программа позволяет моделировать (создавать) ситуации различного уровня сложности, редактировать их, прикреплять дополнительный контент (фото-, видео-, аудиоматериалы), что обозначает возможность постепенного повышения компетенции и решения все более сложных следственных задач сотрудниками. В программе также представлены готовые задания двух видов: «Обучение» (с пошаговыми инструкциями) и «Экзамен». Задания из разряда «Обучение» позволяют быстро получить необходимые навыки работы с тренажером, понять его логику, научиться работать с криминалистической техникой. Контроль же знаний возможно провести в режиме реального времени на любом этапе выполнения заданий. Для оперативного разрешения возникших в процессе обучения непонятных моментов существует раздел «Вопросы», в кото-

ром можно найти ответы на наиболее часто задаваемые вопросы или сформулировать свой собственный и получить на него ответ в наиболее короткий срок. Также полезной функцией является возможность сохранять персональные результаты учащегося/тестируемого, что позволяет следить за прогрессом обучения, выявить типичные ошибки и предотвратить дальнейшее их появление.[1]

Пока данное программное обеспечение представляет собой лишь своеобразный тренажер и носит больше обучающий характер, но в перспективе эта разработка обещает стать существенным подспорьем практикующим работникам. Вскоре громоздкие очки и джойстик не понадобятся, их обещает заменить 3D-приложение для смартфона, планшета и любого другого переносного гаджета. Так, следователь непосредственно на месте происшествия будет через видеоролик создавать реконструкцию, которая в дальнейшем при помощи программ будет преобразовываться в 3D-модель, и исследование места происшествия можно будет уже производить непосредственно в ней. Однако все эти инновации только будут ожидать следственные органы в будущем.

В настоящее время разработки по совершенствованию программы продолжаются. Полученные технологии будут иметь важное значение на первоначальном этапе расследования по таким общественно-значимым преступлениям, как теракты, транспортные преступления, техногенные катастрофы.

Что касается работы специалиста-криминалиста, то в его деятельности также необходимо развитие компьютерного моделирования, которое уже на месте происшествия либо вне его позволит решать различные идентификационные и диагностические вопросы без необходимости использования улик.

Так, в практике судебно-медицинской деятельности уже используются программы компьютерного моделирования, которые позволяют проработать все возможные сценарии действий лиц на месте преступления, а также при помощи иллюстративности материала наглядно и аргументированно преподнести доказательственную информацию органам расследования и суду. Отдельного внимания заслуживают пакеты трехмерного моделирования и анимации Maya, Autodesk 3DS Max, Blender 2.61 Poser и др.[2]

---

[1] *Гармаев Ю.П.* Проблемы и перспективы внедрения высоких технологий в криминалистические, межотраслевые средства противодействия преступности // Вестник Бурятского Государственного Университета. 2014. № 2. С. 98–107.

[2] Верстак, В. 3 d s Max 2008. СПб., 2008. С. 252.

Например, пакет Autodesk 3DS Max содержит модуль Character Studio, представляющий собой средство для анимации персонажей и состоящий из двух независимых модулей Biped (создание и анимация скелета) и Physique (модификатор, позволяющий связать скелет с сетчатой полигональной оболочкой персонажа). Данная программа позволяет применять параметры скелета человека. Наличие взаимосвязанного комплекса суставов и их связь с условным центром тяжести, а также воспроизведение реалистичных движений человека в соответствии с законами гравитации визуально, соответственно предлагаемым ситуациям взаиморасполагать в трехмерном пространстве сами фигуры моделей, их отдельные фрагменты, вносить в сцену условные орудия совершения преступления и многое другое позволяет решать большой круг вопросов, вынесенных на разрешение перед экспертом. Возможность «создания» скелета с учетом метрической системы измерений позволяет производить сопоставление моделей в сцене с учетом реального роста участников событий. Отдельного внимания заслуживает то обстоятельство, что после подготовки сцены и ее предварительной визуализации сохранять на электронные носители можно файлы, фиксирующие как отдельные моментные условия событий в виде растровых изображений, так и развитие динамики событий с сохранением в видеофайл.[1]

Данные программные продукты позволяют как самому эксперту дать ответы на вопросы, задаваемые в процессе экспертизы, так и при помощи наглядных графических схем наглядно продемонстрировать доказательственное заключение и исключить иные варианты образования следов и т. д. Так, практике известен случай, когда в судебном заседании подсудимый заявил об обстоятельствах причинения повреждений потерпевшему при условии, когда тот сам наткнулся на нож во время нападения на обвиняемого, у которого в руке было данное орудие. При исследовании трупа установлено, что колото-резаная рана располагается на передней поверхности брюшной стенки, в эпигастральной области, направление раневого канала спереди назад, сверху вниз. При допросе эксперту был задан вопрос о возможности образования повреждения при указанных подсудимым условиях. Наличие схем, иллюстрирующих указанную экспертизу, выполненных в графическом редакторе 3ds max, позволило исключить такой вариант их образования.[2]

---

[1] *Кулагин Б.С.* Актуальное моделирование, визуализация и анимация в 3 d s Max 7.5. СПб., 2005. С. 444–449.

[2] Судебно-медицинская фотография: современные аспекты: метод. рекомендации / В.В. Колкутин, С.В. Леонов, И.В. Власюк, Н.И. Шишканинец. М.: Рос. центр судеб.-мед. экспертизы, 2011. 144 с.

Однако стоит отметить, что сфера применения программных комплексов, используемых в судебно-медицинской экспертизе, весьма широка (кинематография, мультипликация, компьютерные игры, архитектура, инженерия и многое другое). В настоящее время специализированные криминалистические пакеты, которые без использования специальный знаний компьютерного моделирования позволят экспертам реконструировать место происшествия и отдельные его фрагменты, отсутствуют. При этом очевидно, что упрощение модулей и плагинов, а также их криминалистическая специализация может оказать существенную помощь экспертам и другим участникам следственных действий в устранении пробелов, связанных с недостаточностью документальных сведений, иллюстрирующих варианты развития событий совершения преступлений (фототаблиц, схем, видеофрагментов и др.), предлагаемых на разрешение ситуационных криминалистических экспертиз.

Хочется надеяться, что такого рода программные комплексы появятся в экспертной и следственной практике в ближайшем будущем. Данные программные средства могут значительно облегчить работу криминалистов и существенно повысить эффективность и качество расследования и, в конечном итоге, обеспечить надлежащий уровень защиты прав и законных интересов всех участников уголовного судопроизводства[1].

---

[1] *Яковлева А. В., Алабердеев Р. Р., Андросов С. М., Афицинский В. А., Бабак Ю. Н., Баширова Н. В., Беспалько А. А., Бойко М. В., Бурбело О. А., Быкова К. В., Гапоненко А. В., Гассий В. В., Герасимов А. В., Головко М. В., Долинко В. И., Еськов С. В., Злобина И. В., Калинина Н. Н., Камкия Б. А., Кизим А. А. и др.*: Механизм экономико-правового обеспечения национальной безопасности: опыт, проблемы, перспективы. Краснодар, 2012.

Криминалистика в цифровой век

В. А. Мещеряков,
профессор кафедры,
доктор юридических наук,
кандидат технических наук, профессор
(Воронежский государственный университет)

В статье рассматривается влияние элементов современного информационного общества на содержание науки криминалистики.

Криминалистика, информационные технологии, кибернетическое пространство интернет-вещей, Большие данные.

Почти 20 лет мы уже живем в новом XXI веке и новом тысячелетии, в которые человечество вошло с богатым набором прорывных технологий. В первую очередь это радиоэлектроника, ядерная энергетика, космическая техника, генная инженерия и целый ряд других.

Однако безусловным локомотивом всех этих изменений стало развитие новых информационных технологий, создание на их основе компьютерной техники и повсеместное ее внедрение практически во все сферы человеческой жизни.

Следует сказать, что криминалистика не осталась в стороне от этого процесса и прошедшие 20 лет – уже достаточный срок для того, чтобы взглянуть на то, как изменилась современная криминалистика под влиянием бурно развивающихся информационных технологий.

Как и положено, значительную помощь в осмыслении происходящих перемен для криминалистики оказало уголовное право. С принятием в 1996 г. действующего Уголовного кодекса мы получили принципиально новые объекты уголовно-правового регулирования: компьютерную информацию, вредоносные компьютерные программы, критическую информационную инфраструктуру. Названные объекты, а также компьютеры всех калибров и назначений, цифровые сети связи, развернутые на их основе информационные системы и сервисы образовали специфическое «кибернетическое пространство», в котором протекает значительная часть жизни современного человека.

При этом анализ этой новой среды кибернетического пространства показал, что оно обладает целым рядом криминалистически значимых свойств.

1. Современный человек уже неотделим от комплекса технических устройств, которые он либо:

– носит с собой (мобильные телефоны, гаджеты);

– попадает в их сферу действия (камеры видеонаблюдения, базовые станции мобильной связи);

– постоянно обращается к ним (социальные сети и различные интернет-ресурсы);

– ежедневно использует их в своем быту и повседневной деятельности (умный дом, умный город, «Интернет вещей»).

В результате подробный анализ названных элементов может очень много сказать о человеке, который взаимодействует с ними. Например, существует точка зрения, что привычный мобильный телефон это ни много ни мало – частичка личности его владельца. Так, список контактов, хранимый в памяти телефона, даст нам круг общения, а частота и направление входящих и исходящих звонков позволит выявить перечень самых близких людей. Изображения-аватарки и мелодии вызова, назначенные каждому из контактов, позволяют оценить эмоциональное отношение к нему владельца телефона. Фотографии и их географические метки, треки местоположения и их повторяемость в различные дни и время суток позволит с высочайшей вероятностью выявить места жительства, работы, а также массу дополнительной очень личной для каждого человека информации. Специалисты этот перечень смогут легко продолжить.

2. Все технические устройства, используемые человеком, принципиально могут содержать в себе (а сейчас с большой вероятностью говорить, что уже содержат) связные элементы (приемопередатчики), позволяющие подключать их к цифровым сетям связи и осуществлять взаимодействие между собой. Круг таких предметов и используемых протоколов взаимодействия очень разнообразен. Это телевизоры, холодильники, кондиционеры, видеокамеры, часы, кардиографы, шагомеры, пульсометры и т. п. Теперь даже осветительные лампочки и столовые приборы уже способны на это. Все эти предметы начинают взаимодействовать между собой (зачастую в автоматическом режиме без участия человека) и пытаются подстроить режимы своей работы к привычкам и особенностям своего хозяина – конкретного человека. Уже сложился термин «Интернет вещей», отражающий подобную ситуацию, в которой мы начинаем жить.

При этом возникшее кибернетическое пространство представляет собой не просто совокупность отдельных технических объектов, способных воспринимать следы активности человека (о чем говорилось чуть ранее), а уже образует плотно связанную

и взаимодействующую среду, в которой криминалистически значимые отражения (фактически следы) могут преобразовываться, копироваться и передаваться от одного устройства к другому. В результате эти следы за счет множества локальных взаимодействий начинают передаваться на огромные расстояния и храниться в цифровом виде в неограниченном количестве мест и практически неограниченное время.

3. Благодаря тому, что сегодня практически все устройства используемые человеком, содержат в своем составе как минимум микроконтроллер и связной блок, они генерируют, хранят и передают разнообразную информацию различных форматов (изображения, звуки, телеметрия и т. п.). Все это хранится достаточно долго, образуя просто гигантские объемы информации, измеряемые числами космического масштаба. Самое удивительное, что современные технические возможности позволяют работать со всем этим объемом и извлекать из него очень ценные результаты, необъяснимые простым качественным анализом и не вытекающие из знания какой-либо понятной закономерной взаимосвязи.

Для этого явления наукой предложено специальное понятие «Большие данные», определяемое как информационные технологии и архитектуры нового поколения для экономичного извлечения ценности из разноформатных данных большого объема путем их быстрого захвата, обработки и анализа.

Все перечисленные особенности привели к тому, что криминалистика была вынуждена исследовать особенности этих объектов, изучать специфику механизмов следообразования с их участием, проводить анализ того, как они видоизменили способы совершения «традиционных» преступлений.

Первое, о чем следует сказать в данном контексте, это формирование новой категории следов – виртуальных, которые занимают промежуточное положение между традиционно выделяемыми материальными и идеальными следами.

Их принципиальное отличие в том, что они сохраняют в себе отражение не свойств следообразующих объектов, а всего лишь фиксируют значения параметров формализованной (математической) модели, которая была положена в основу создания технического устройства для регистрации реальной действительности.

Например, если при фиксации окружающей действительности на кинопленку мы могли всю временную цепочку разбить на интервалы в 1/24 секунды и на полученных кадрах для каждой точки окружающей обстановки поставить в соответствие участок

на кинопленке, то для цифровой видеозаписи такого соответствия получить не удастся. Это обусловлено в первую очередь тем, что необходимых 24 кадров на видеозаписи реально не существует. Есть базовый кадр, записанный с использованием различных технологий сжатия видеоданных, и некие параметры, характеризующие отличие базового кадра от изображения в текущий момент времени. При этом когда возникает необходимость воспроизвести изображение в заданный момент времени, используется базовый кадр, по которому с помощью записанных параметров формализованного описания изображения вычисляются необходимые видеоданные и на их основе отрисовывается нужная картинка.

Эти достаточно необычные для традиционной криминалистики виртуальные следы в своей совокупности формируют целый ряд новых объектов (например, таких как электронные документы, торрент-файлы, виртуальные машины, полиморфные компьютерные программы и т. п.), обладающих уникальными криминалистическими свойствами, абсолютно не вписывающимися в традиционные представления.

Казалось бы, самое простое и наиболее понятное – электронные документы на сайтах в сети Интернет. Первое впечатление, что цифровые технологии ничего не изменили, кроме формы представления символов. Раньше буквы были на бумаге, а теперь буквы на экране монитора возникают из кодов, где каждому коду соответствует своя буква.

Если посмотреть глубже, то увидим, что говорить об однозначном соответствии бумажного и электронного документа вообще нельзя. Можно ставить вопрос только об их функциональной эквивалентности. Похожего по виду на бумажный документ электронного документа в виде единого объекта (файла или набора данных) может вообще не существовать. Технология CMS (систем управления содержимым) позволяет создавать визуальное представление электронного документа из отдельных фрагментов (фрагментов текстовых строчек, фона страницы, используемых иллюстраций и даже небольших программ-макросов), что называется, на лету в ходе просмотра документа человеком. При этом используемые фрагменты могут храниться в разных файлах, на разных физических дисках, в разных компьютерных системах, географически расположенных даже на разных континентах.

Другой уникальный с точки зрения криминалистики объект – пиринговые сети и торрент-файлы[1]. Многие преступления,

[1] BitTorrent (протокол) // Википедия. [2018–2018]. Дата обновления: 07.05.2018. URL: https://ru.wikipedia.org/?oldid=92510307 (дата обращения: 07.05.2018).

предусмотренные ст. 146 УК Российской Федерации, тесно связаны с этими объектами.

При распространении объекта, охраняемого авторским правом (видеофильмы, литературные произведения, аудиозаписи), исходный файл разбивается на большое количество частей и благодаря посредничеству торрент-трекера множественными сессиями начинает передаваться в пиринговую сеть. Абоненты сети, получив торрент-файл, начинают выкачивать части распространяемого видеофильма/аудиозаписи, одновременно становясь точками раздачи тех фрагментов, которые уже успели скачать целиком. Адреса абонентов сети, у которых уже имеются части распространяемого объекта, динамически отражаются на торрент-трекере. Убедившись в том, что все части распространяемого объекта уже скачаны хотя бы одним абонентом сети (пиром), субъект, начавший распространение объекта, может вообще отключиться от компьютерной сети.

В результате складывается уникальная в криминалистическом плане ситуация. Все части распространяемого объекта имеются в сети, но ни один из абонентов сети не имеет всего этого объекта целиком. Однако благодаря торрент-трекеру он будет знать, где размещены части целого объекта, и может «воспользоваться его полезным качеством» (например, просмотреть видеофильм или прослушать аудиозапись), последовательно скачивая из известных мест (подключенных к сети пиров) необходимые в каждый момент времени фрагменты для непрерывного воспроизведения и удаляя их у себя сразу же после использования.

Еще один уникальный криминалистический объект обязан своим появлением идеям виртуализации вычислительных систем. В основе этого явления лежит постулат о том, что для любой технической системы может быть создана компьютерная программа, полностью имитирующая все тонкости ее функционирования. При этом в качестве имитируемой системы может выступать такой же компьютер, как и тот на котором моделирующая программа запущена. Поскольку имитирующая программа (виртуальный компьютер) ничем не отличается по своим свойствам от реального компьютера, то в ее среде может быть запущена любая иная программа, в том числе и еще один (фактически вложенный) виртуальный компьютер. При этом глубина вложения виртуальных компьютеров будет ограничиваться только техническими характеристиками реального компьютера, на котором запущена вся эта система виртуализации.

С криминалистической точки зрения в данном случае мы получаем очень сложную многоуровневую следовую картину, в которой один след вложен в другой и на каждом уровне этой иерархии могут проявляться свои особенные связи с событием преступного деяния.

Приведенный перечень необычных криминалистических эффектов, возникающих в результате внедрения в повседневную жизнь человека современных телекоммуникационных и информационных технологий, далеко не исчерпывающий и его можно легко продолжить. Подробное их изучение и включение в существующую систему научных знаний – актуальная задача современного этапа развития криминалистки.

Базы данных автоматизированных систем бухгалтерского учета как объекты исследования судебных бухгалтерских экспертиз по уголовным делам

Ю. Ю. Миленина,
эксперт
(ЭКЦ МВД России)

В статье рассматриваются проблемы исследования баз данных автоматизированных систем бухгалтерского учета в процессе судебно-бухгалтерской экспертизы в МВД России.

Судебная бухгалтерская экспертиза, объекты экспертного исследования, преступления экономической направленности, базы данных автоматизированных систем бухгалтерского учета.

В настоящее время в ходе выемок проводится изъятие компьютеров, серверов, электронных носителей информации либо производится выгрузка базы данных учета (копирование на иные электронные носители) ввиду полного или частичного отсутствия документов на бумажных носителях. Тактика изъятия баз данных достаточно изучена, а также процесс придания юридической силы и приобщения их к материалам дела.

В случае необходимости решения вопросов по формированию доказательственной базы в ходе расследования путем производства судебной бухгалтерской экспертизы возникает вопрос возможности использования данных объектов для дальнейшего исследования.

В настоящее время в теории и практике производства судебных экономических экспертиз к основным объектам исследования относят: первичные учетные документы; иные первичные документы, используемые при ведении учета; регистры бухгалтерского учета, регистры налогового учета, регистры учета индивидуального предпринимателя и т. п.; бухгалтерская отчетность; налоговые декларации; иные материалы уголовного дела, содержащие фактические данные, относящиеся к предмету экспертизы[1].

Они представляются на экспертизу как на бумажных носителях, так и на электронных носителях, исключающих возможность

[1] *Мусин Э. Ф.* Судебно-экономическая экспертиза в уголовном процессе: практическое пособие. М.: издательство Юрайт, 2017. С. 29.

внесения изменений (например, на оптических носителях – дисках формата CD-R (DVD-R) с отсутствием возможности перезаписи) и имеющие признаки идентификации (например, номер вокруг посадочного отверстия).

Широко используются субъектами экономической деятельности для ведения бухгалтерского учета различные автоматизированные системы учета, системы управления базами данных. Наиболее распространенным в России является «1С:Предприятие» в конфигурации «1С:Бухгалтерия».

Согласно действующим нормам законодательства:

– эксперт вправе давать заключение в пределах своей компетенции, в том числе по вопросам, хотя и не поставленным в постановлении о назначении судебной экспертизы, но имеющим отношение к предмету экспертного исследования (п. 4 ч. 3 ст. 57 УПК РФ);

– эксперт не вправе самостоятельно собирать материалы для экспертного исследования, а также проводить без разрешения лица, назначившего экспертизу, исследования, могущие повлечь в том числе изменение их внешнего вида или основных свойств (п. 2 и 3 ч. 4 ст. 57 УПК РФ, а для государственных судебных экспертов – ст.16 ФЗ №73-ФЗ от 31.05.2001);

– государственный эксперт проводит исследования объективно, на строго научной и практической основе, в пределах соответствующей специальности, всесторонне и в полном объеме (ст. 8 ФЗ № 73-ФЗ от 31.05.2001).

Извлечение данных из информационных баз для проведения судебной экономической экспертизы (по их родам и видам) обычно осуществляется специалистом в ходе следственных действий, а экспертом уже проводится их исследование в процессе производства судебной экономической экспертизы. Но в последнее время встает вопрос исследования информационных баз без привлечения специалиста, сразу в ходе проведения судебной экономической экспертизы экспертом.

Так, если база данных содержится на диске одноразовой записи, переведенном в режим чтения, любая иная запись на него будет под запретом. Эксперт не сможет своими действиями при работе с базой данных повлечь изменения свойств представленных на исследование объектов. Однако если база данных содержится на иных цифровых запоминающих устройствах, невозможно утверждать, что заинтересованными лицами не будут внесены изменения, которые приведут к искажению/утере/порче учетных данных, что ставит под сомнение возможность исследования данных объектов экспертом. Однако, по мнению автора, при соблюдении органом/лицом,

назначившим экспертизу, требований ст. 87 и ст. 88 УПК РФ в рамках оценки доказательств на относимость, допустимость и достоверность, соблюдение иных процессуальных требований, экспертом возможно использование данных объектов (с соблюдением определенных требований).

Также необходимо отметить, что в рамках судебной бухгалтерской экспертизы можно исследовать и устанавливать лишь отраженные в учетной документации факты финансово-хозяйственной деятельности, а также данные об имуществе и обязательствах хозяйствующих субъектов.

Однако не стоит забывать, что законодательством в сфере бухгалтерского учета предусмотрено оформление каждого факта хозяйственной жизни первичным учетным документом, а в последующем – их регистрация и накопление в регистрах бухгалтерского учета и систематизация в отчетности, регламентированы требования к их составлению (реквизиты и т. д.).

В характеристике программного продукта «1С:Бухгалтерия» отражено, что бухгалтерский и налоговый учет в системе построен в соответствии с действующим законодательством РФ, а значит работа с ней осуществляется на основе специальных знаний в области бухгалтерского учета и общих навыков работы с программными средствами.

В автоматизированных базах учета данные изначально не представлены в виде документа бухгалтерского учета, они извлекаются после использования общих и/или нестандартных приемов программных продуктов экспертом/специалистом в ходе проведения исследования.

Общие приемы извлечения данных предусмотрены разработчиками программного обеспечения, описание их содержится в инструкциях к эксплуатации и прочей технической документации (например, формирование стандартных отчетов в программе 1С). Необходимо отметить, что экспертная задача должна стоять таким образом, чтобы у эксперта была возможность идентифицировать в представленной информационной базе конкретный исследуемый факт хозяйственной жизни. Для арифметических расчетов наиболее удобны форматы файла, пригодные для работы в программе Excel, вследствие чего возникает необходимость выгрузки сформированных в исходном программном продукте ведения учета документов, отчетов, сводных таблиц данных и прочего в необходимый формат. Например, в 1С после формирования отчета «Карточка счета» за исследуемый период с различными аналитическими отборами (по контрагенту, по договору и т. д.), возможно сохранение

файла в нужный формат. Указанная тактика в основном применяется специалистами в ходе следственных действий в целях оказания содействия в изъятии документов для последующего предоставления данных объектов на судебную экономическую экспертизу.

Нестандартные приемы извлечения данных предусматривают применение частных экспертных методик. Следует отметить, что здесь могут требоваться знания и навыки не только в области экономических наук, но и, например, в области информационных технологий и т. п.

Существует позиция, что при наличии необходимости при проведении одного исследования не только специальных познаний в области экономических наук, но и в области компьютерной техники, программирования и т. п., следует назначать комплексную экспертизу. Но так как развитие информационных технологий влияет и на изменение форм представления данных бухгалтерского учета, назревает необходимость совершенствования экспертных методик, повышение компетенции экспертов экономистов в области информационных систем (автоматизированных систем бухгалтерского учета, работы с базами данных этих систем)[1].

Выше отмечалось, что, как правило, автоматизированные системы ведения бухгалтерского учета строятся на основе требований к бухгалтерскому учету и законодательства, поэтому любая работа с программой подразумевает участие специалиста в соответствующей области. Так как судебная экспертиза подразумевает проведение именно исследования, нужно сказать, что в область задач судебно-экономических экспертиз не могут входит справочные вопросы, относимые к сведениям, содержащимся в базах данных автоматизированных систем бухгалтерского учета. Например, установление перечня контрагентов исследуемого лица, или списка наименований товаров, отраженного в информационной базе по операции поступления материально-производственных запасов по конкретному документу. Данные задачи могут быть решены привлечением специалиста, который в письменной форме (заключение специалиста) высказывает собственное суждение по справочным вопросам, поставленным перед ним следователем, а не проведением экспертизы. Но, например, вопрос «Каким образом отражена в информационной базе поставка товара по договору № Х от ХХ.ХХ.ХХ за период с Х по Х и на какую сумму?» уже является задачей судебной бухгалтерской экспертизы.

Таким образом, в целях проведения исследования информационных баз автоматизированных систем ведения бухгалтерского

[1] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

учета объективно, на строго научной основе, в пределах соответствующей специальности сформированы следующие рекомендации по работе эксперта с данным объектом исследования:

1) объекты исследования должны быть оценены следователем с точки зрения допустимости, относимости и достоверности;

2) должны представляться на электронном носителе, с отсутствием возможности внесения изменения в содержащиеся на нем данные – например, на неперезаписываемых CD-R (DVD-R) дисках с указанием номера вокруг посадочного отверстия диска; сведений о невозможности внесения в содержащиеся на дисках данные изменений программными средствами; полное наименование содержащихся на диске файлов, их формат, пароли и (или) имена пользователей (при их наличии) для беспрепятственного доступа к данным, содержащимся в файлах; сведения о содержащихся в файлах данных; при наличии множества папок – путь к исследуемым файлам; при наличии нескольких баз данных (файлов), содержащих идентичные/однотипные сведения, но имеющих расхождения в отраженных в них данных, – информацию о базе данных (файле), данные которых необходимо использовать в качестве исходных при производстве экспертизы;

3) описание программного обеспечения, с помощью которого ведется работами с базами данных (версия, конфигурация и т. п.);

4) наличие лицензионного программного обеспечения для работы с соответствующей информационной базой;

5) предоставление кода доступа к соответствующей базе данных с необходимыми для исследования правами пользователя системы;

6) техническая документация (руководство к пользованию и т. п.) по конкретному программному обеспечению;

7) предоставление учетной политики исследуемого лица и/или пояснения лица, ведущего учет в автоматизированной системе, об отражении конкретных интересующих фактах хозяйственной жизни (использование для учета субсчетов, порядок формирования/расчета конкретных показателей, особенности учета и прочее);

8) наличие достаточных рабочих мощностей (для работы с массивными базами данных);

9) экспертная задача должна стоять таким образом, чтобы была возможность идентифицировать в представленной информационной базе конкретный исследуемый факт хозяйственной жизни;

10) описание этапов исследования представленных объектов: порядок действий по формированию отчетов/документов, по извлечению данных с возможной иллюстрацией снимками экрана.

О некоторых проблемах организации борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий

А. В. Морозов,
кандидат юридических наук
(ГУНК МВД России)

В статье рассматриваются современные проблемы выявления и раскрытия преступлений в сфере незаконного оборота наркотиков, совершенных с использованием ИК-технологий.

Борьба с незаконным оборотом наркотиков, Интернет, законодательство, Главное управление наркоконтроля, МВД России.

Проводимый Главным управлением по контролю за оборотом наркотиков МВД России (далее – ГУНК) анализ наркоситуации показывает, что на протяжении последних пяти лет наркорынок в России претерпевает серьезные негативные изменения. Удельный вес «синтетики» в общей массе изымаемых наркотических средств и психотропных веществ на протяжении последних 10 лет увеличился в 13 раз и по итогам 2017 г. составил 26,1 % (5,6 т). В незаконном обороте наряду с традиционными стимуляторами амфетаминового ряда (метамфетамин, МДМА, амфетамин) особое распространение получили относительно новые виды наркотиков (N-метилэфедрон, мефедрон и их производные, синтетические аналоги тетрагидроканнабинола (курительные смеси), наркотические средства фентаниловой группы (например, карфентанил). Аналогичная проблематика обозначена и в докладах МККН ООН.

Отличительной особенностью типичной современной преступной схемы сбыта синтетических наркотиков является их бесконтактный способ распространения, основанный на использовании новейших технологий в информационно-коммуникационной среде. Интернет рассматривается не только как огромная рекламная и пропагандистская площадка, но и как средство коммуникации, вербовки продавцов и курьеров, способ и место сбыта наркотиков.

Для размещения объявлений о магазинах, торгующих наркотическими средствами, используются специализированные так называемые «нарко-форумы», где любой желающий за определенную плату может разместить рекламу о продаже наркотических средств, их видах, ценах, способах приобретения и ссылку на свой интернет-

сайт. На указанных форумах любой из зарегистрированных там пользователей может участвовать в обсуждении тех или иных видов наркотиков и оценке деятельности представленных интернет-магазинов. Самыми крупными подобными тематическими интернет-форумами являются «LegalRC» и «Wayaway», серверы которых недоступны для технического контроля.

С конца октября 2016 г. неустановленными лицами, предположительно являющимися организаторами «LegalRC» и «Wayaway», создана крупнейшая на постсоветском пространстве торговая площадка «HYDRA» (400 магазинов). Сделки и оплата происходят непосредственно на площадке, охвачены все сферы теневого бизнеса: от продажи наркотиков до торговли поддельными документами, банковскими картами, оформленными на подставные данные, специальным оборудованием для слежки и съема информации, а также предоставления различных информационных услуг. Суточный торговый оборот – около 7 млн долл. США. Получаемые денежные средства дают возможность организаторам привлекать к своей деятельности высококлассных специалистов по информационной безопасности, экспертов «химиков», врачей наркологов, юристов, а также бывших сотрудников правоохранительных органов.

Инструментом наркосделок на данных площадках становятся различные электронные платежные системы и сервисы («QIWI-банк», «ЯндексДеньги», «WebMoney», «E-port»). Указанные в объявлениях электронные кошельки и почтовые адреса, номера телефонов оформляются на вымышленных лиц или по поддельным документам. Используемые номера абонентов сотовой сети, как правило, являются виртуальными и не имеют привязки к физическому лицу.

В последнее время покупка наркотиков осуществляется через интернет-биржи обмена криптовалюты «Биткоин».

Передача (сбыт) наркотиков покупателям осуществляется посредством адресных «кладов», «тайников» или «закладок». Как правило, так называемые «кладчики» для сокрытия наркотиков сами выбирают места (подъезды домов, гаражи, столбы, скрытые полости объектов и предметов, находящихся на улице). При этом потребители, наркокурьеры и продавцы друг с другом никогда не видятся, для связи используют определенные социальные сети или мессенджеры.

Существует два основных типа распространения наркотических средств через сеть Интернет:

1) через интернет-сайты автоматических продаж

2) с использованием программ для мгновенного обмена сообщениями.

Кроме того, программы-мессенджеры используются для организации спам-рассылок с рекламой указанных магазинов и способов обхода блокировки. Для привлечения новых и удержания постоянных клиентов проводятся специальные маркетинговые акции, осуществляются бесплатные доставки «пробников», предоставляются скидки и т. п.

В данных системах прослеживается ступенчатая иерархия. Все функции участников преступной деятельности четко распределены, соблюдается жесткая дисциплина, продумана система безопасности, на которую щедро тратятся полученные от наркобизнеса доходы. В такие преступные структуры обычно входят «закладчики» различных уровней, «вербовщики», «кладовщики», «курьеры», «операторы», «финансовый директор», программисты, координаторы, диспетчеры, финансисты, кассиры, легализаторы, химики. Хорошо зарекомендовавший и проявивший себя в работе сотрудник переводится на вышестоящие должности с увеличением заработной платы. В отношении «персонала», допустившего нарушения, применяются штрафные санкции. Каждый сотрудник получает развернутые инструкции, в которых подробно описано, как правильно фасовать, хранить и перевозить наркотические средства, делать «закладки», общаться с потребителями наркотиков, как безопасно пользоваться электронными счетами и обналичивать денежные средства, как пользоваться анонимными средствами передачи информации через Интернет и анонимными иностранными прокси-серверами при посещении интернет-страниц и в общении между собой, как вести себя в случае задержания сотрудниками правоохранительных органов и т. д. Ряды нижестоящих звеньев постоянно пополняются посредством ведения грамотной «вербовочной» работы в Интернете, обещанием высокого дохода при минимальных временных затратах.

Подобные схемы сетевого наркобизнеса существенно затрудняют установление личностей наркодельцов и формирование доказательственной базы их причастности к преступной деятельности.

В результате проведенного анализа установлено, что в России действуют более 10 тыс. интернет-ресурсов (в том числе автомагазины, каналы в мессенджере «Telegram»), посредством которых осуществляется сбыт наркотиков.

Напомню: в 2012 г. в России создан Единый реестр сайтов, доступ к которым блокируется Роскомнадзором[1]. ГУНК организо-

[1] О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в инфор-

вана работа по оценке размещенной на сайтах информации о наркотиках. Так, в 2017 г. ГУНК рассмотрено более 46 тыс. электронных обращений Роскомнадзора, по которым принято 19 432 решений об ограничении доступа к интернет-сайтам и страницам в социальных сетях, располагающим запрещенной информацией о способах, методах изготовления, использования наркотиков, местах их приобретения.

Исходя из мирового опыта и в связи с несовершенством законодательства, само по себе прекращение деятельности интернет-ресурсов не приводит к сокращению объема наркоторговли, поэтому основные усилия сотрудников наркоконтроля направлены на пресечение каналов поставок наркотиков, ликвидации организованных групп и преступных сообществ, занимающихся их изготовлением и сбытом. Руководством МВД России обращено особое внимание на эти проблемы. В 2017 г. пунктом 4.5 ПООМ МВД России ГУНК поручено организовать комплекс мероприятий по выявлению и пресечению деятельности участников преступных группировок, занимающихся распространением подконтрольных веществ бесконтактным способом при помощи сети Интернет.

В результате проведенных мероприятий ОВД выявлено 7 179 наркопреступлений, совершенных с использованием интернет-технологий, возбуждены уголовные дела в отношении 3 069 лиц, причастных к их совершению, из незаконного оборота изъято свыше 1 т 976 кг наркотиков. Прекращена незаконная деятельность 654 российских интернет-ресурсов (форумы, магазины автоматических продаж, телеграм-каналы). Активная работа сотрудников наркоконтроля привела к ликвидации в августе 2017 г. крупной интернет-площадки по продаже наркотиков «RAMP», на которой размещалась реклама более 33 оптовых и 121 розничных магазинов.

Так, в 2015–2016 гг. одним из основных игроков на российском наркорынке с годовым оборотом 2,3 млрд рублей являлся международный интернет-магазин «ХимПром». Было налажено производство синтетических наркотиков в трех подпольных лабораториях производительностью от 150 до 500 кг в неделю, созданы оптовые склады в 10 регионах РФ. С целью сбыта наркотиков преступники организовали структурные подразделения в 14 регионах, наладили логистическую цепочку, включающую в себя доставку особо круп-

---

мационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено»: постановление Правительства РФ от 26 октября 2012 г. № 1101 [Электронный ресурс]. URL: https: //eais.rkn/gov/en/feedback (дата обращения: 18.04.2018).

ных партий наркотических средств в специально оборудованных тайниками автомашинах. Расчеты осуществлялись с использованием различных криптовалют и электронных платежных систем. В результате проведенных мероприятий задержаны 67 участников наркогруппировки, 47 из которых являются гражданами Украины. Из незаконного оборота изъято свыше 4 т синтетических наркотиков, 3,5 т прекурсоров, 250 единиц лабораторного оборудования, 2,5 млн рублей, 18 общегражданских паспортов РФ с признаками подделки, 9 автомашин, оборудованных тайниками.

В 2015 г. в российском интернет-пространстве появился новый магазин под брендом «Stuff.store», созданный для распространения на территории РФ оптовых партий синтетических наркотиков. Организаторами был налажен весь цикл оборота наркотических средств от производства до сбыта конечному потребителю. Вербовка участников осуществлялась через социальные сети путем размещения объявлений о приеме на высокооплачиваемую работу в качестве закладчиков и курьеров. С целью сбыта наркотиков организаторами сформированы структурные подразделения группировки в 10 регионах РФ, налажена логистическая цепочка, включающая в себя доставку особо крупных партий наркотических средств в оборудованных тайниками автомашинах. Расчеты осуществлялись с использованием криптовалют. К 2017 г. группировка стала одним из самых крупных «игроков» на российском наркорынке.

В январе – феврале 2018 г. ГУНК совместно с региональными подразделениями деятельность межрегиональной организованной преступной группы пресечена. На территории Московской, Новосибирской, Челябинской областей, а также Хабаровского края выявлены и ликвидированы четыре нарколаборатории, производительность которых составляла от 20 до 100 кг синтетических наркотиков в неделю. Пресечена деятельность 5 структурных подразделений. Задержано 27 участников наркогруппировки. Из незаконного оборота изъято более 345 кг синтетических наркотических средств, 500 кг различных химических реактивов, используемых при изготовлении наркотиков, 87 единиц лабораторного оборудования.

В 2018 г. прогнозируется увеличение количества наркопреступлений, совершенных с использованием информационно-телекоммуникационных технологий, поэтому ГУНК и территориальными органами МВД России на региональном уровне осуществляется комплекс мероприятий, направленных на выявление и пресечение деятельности организованных групп и преступных сообществ, занимающихся распространением наркотических средств и психотроп-

ных и сильнодействующих веществ с использованием информационно-телекоммуникационных технологий.

Успех работы на данном направлении зависит от целеустремленности и профессиональной грамотности полицейских, а также слаженного взаимодействия с другими службами и организациями. Профессиональную грамотность наши сотрудники повышают на специальных курсах в Академии управления МВД России и ВИПК МВД России. Кроме того, разработаны и внедрены в практику научно-практические работ. В настоящее время Академией управления МВД России по заявке ГУНК готовятся методические рекомендации «Документирование преступной деятельности лиц, причастных к легализации наркодоходов, в том числе с использованием интернет-бирж обмена криптовалюты».

По инициативе ГУНК в совместную работу вовлечены ФГУП «Главный научно-исследовательский вычислительный центр Управления делами Президента Российской Федерации», Росфинмониторинг, Ростелеком, службы безопасности банков, платежных систем, «Почта России», транспортные компании, администрации каршеринговых компаний, социальных сетей, бирж криптовалют.

Основной характерной особенностью компьютерных сетей является то, что информация о всех действиях пользователей в них всегда сохраняется. Учитывая это, в практической деятельности ГУНК для выявления и установления участников интернет-магазинов «Даркнета» применяется программное обеспечение «OSINT», позволяющее осуществлять поиск, выбор, сбор и анализ информации из общедоступных источников.

По некоторым вопросам мы используем также онлайн-систему «AIPSIN DRUGS» белорусской компании «БелХард Групп».

В некоторых регионах России создана и внедрена автоматизированная информационная система «Незаконный оборот наркотиков», которая позволяет сопоставлять данные о неустановленном сбытчике и обстоятельствах приобретения задержанным лицом наркотического средства, с указанием используемых при сбыте «ник-неймов», IP-адресов, MAC-номеров, номеров учетных записей в различных программах, электронных платежных системах, банковских счетов, «Киви-кошельках», а также картографических мест закладок наркотических средств и т. п.

В Мурманской области и Удмурдской Республике в 2017 г. на базе ИСОД МВД России созданы ИПС «Дистанционный сбыт наркотических средств».

Мы выступаем с предложениями об объединении всех этих ресурсов и передачи их администрирования в МВД России.

Одной из причин, способствующих росту преступлений в сфере незаконного оборота наркотиков, совершенных с использованием стремительно развивающихся ИК-технологий, является отставание процесса принятия соответствующих законодательных норм.

Так, по нашему мнению, необходима уголовная ответственность лиц, участвующих в создании программного оборудования, используемого для сбыта наркотиков (создание и администрирование интернет-сайтов и страниц в социальных сетях, на которых размещается информация о сбыте наркотиков и психотропов).

Необходимо дополнить УК РФ статьей, предусматривающей уголовную ответственность за пропаганду или незаконную рекламу наркотических средств, психотропных веществ, их прекурсоров или аналогов, растений, содержащих наркотические средства, психотропные вещества или их прекурсоры, либо их частей, содержащих наркотические средства, психотропные вещества или их прекурсоры, инструментов или оборудования, находящихся под специальным контролем и используемых для изготовления наркотических средств или психотропных веществ, способов, методов их изготовления, мест сбыта и немедицинского потребления, а также способов и методов незаконного культивирования растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры (законопроект № 108866-6 рассматривается ГД РФ).

Кроме того, дополнительной уголовной квалификации требует сбыт СДВ и ядовитых веществ (ст. 234 УК РФ), совершаемый с использованием информационно-телекоммуникационных технологий, включая сеть Интернет.

Сегодня главным средством отмывания преступных наркодоходов является криптовалюта (Биткоин, Ethertum и т. д.), анонимность и транснациональность которой в совокупности с активным развитием теневого интернета образуют благоприятную среду для передачи и отмывания наркоденег. По мнению ГУНК, нормативное урегулирование обращения криптовалюты будет способствовать выявлению государственными органами нарушений и перекрытию недобросовестных платежных каналов.

Эти и многие другие вопросы организации выявления и раскрытия наркопреступлений, совершаемых в сфере ИК-технологий нам еще предстоит решить.

Допрос посредством видео-конференц-связи с применением программы «Skype» на стадии предварительного расследования

А. А. Москвичев,
преподаватель кафедры
(Краснодарский университет МВД России)

В статье рассматривается возможность использования систем видео-конференц-связи с применением программы «Skype» на стадии предварительного расследования.

Допрос, свидетель, потерпевший, видео-конференц-связь, «Skype», предварительное расследование.

Научно-технический прогресс, как известно, оказывает влияние на самые разные стороны нашей жизни. Новые технические средства постепенно находят практическое применение и в сфере уголовного судопроизводства, однако темпы их внедрения не всегда отвечают ожиданиям практиков. Сказанное в полной мере относится к использованию систем видео-конференц-связи в российском уголовном процессе, где оно предусмотрено пока лишь в ходе судебных заседаний.

Федеральным законом от 20 марта 2011 г. № 39-ФЗ[1] в УПК РФ внесены изменения, предоставившие право использования средств видео-конференц-связи в ходе судебного разбирательства при допросе свидетеля и потерпевшего по уголовному делу (ч. 4 ст. 240 УПК РФ). При этом правом принятия окончательного решения об организации допроса свидетеля с применением средств видео-конференц-связи оставлено за судом, в чьем рассмотрении находится уголовное дело (ч. 1 ст. 278.1 УПК РФ). Между тем органы предварительного расследования не менее остро нуждаются в возможности дистанционного получения показаний допрашиваемых лиц.

Использование систем видео-конференц-связи не только в суде, но и на стадии предварительного расследования, во-первых, будет способствовать осуществлению уголовного судопроизводства в разумный срок. Во-вторых, производство

[1] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 20 марта 2011 г. № 39-ФЗ // Собр. законодательства Рос. Федерации. 28.03.2011. № 13. Ст. 1686.

допроса при помощи систем видео-конференц-связи в большинстве случаев было бы удобнее и для самих допрашиваемых лиц. В-третьих, использование систем видео-конференц-связи и связанное с ним удобство допроса лица станут мерой, направленной на повышение достоверности даваемых им показаний. В-четвертых, полученные с помощью системы видео-конференц-связи показания, позволят следователю или дознавателю использовать дополнительное (помимо протокольной формы) средство фиксации доказательств – видеозапись произведенного допроса или очной ставки, которое в дальнейшем позволит суду и сторонам убедиться в: а) точности и правильности изложения показаний допрашиваемого; б) разъяснении допрашиваемому прав, обязанностей и ответственности, предусмотренных нормами УПК и УК РФ; в) отсутствии на допрашиваемого физического или психического принуждения со стороны правоохранительных органов. Наконец, в-пятых, использование систем видео-конференц-связи при получении показаний в ходе предварительного расследования позволит отечественным следователям и дознавателям лично (без дополнительной нагрузки на НЦБ Интерпол МВД России) допрашивать лиц, находящихся за пределами Российской Федерации[1].

Как видим, аргументов за расширение возможностей использования систем видео-конференц-связи в российском уголовном процессе достаточно много. Сложности же сводятся, на наш взгляд, главным образом к выбору оборудования и программного обеспечения, необходимого для установки и дальнейшего обслуживания названных систем. В то же время дороговизна первоначальных вложений не должна становиться непреодолимым препятствием на пути совершенствования порядка получения показаний в ходе предварительного расследования.

Действующий УПК РФ допускает возможность применения при производстве следственного действия технических средств (ч. 6 ст. 164, ч.ч. 5, 8 ст. 166 УПК РФ), причем последние исчерпывающе не перечислены. По нашему мнению к таким средствам, помимо фотоаппарата, видеокамеры и т. п., можно отнести программу «Skype».

Как отмечено в литературе, под словом «Skype» («Скайп») обычно понимают как бесплатное программное обеспечение с закрытым кодом, позволяющее осуществлять шифрованную голо-

[1] *Новиков С.А.* Допрос с использованием систем видео-конференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. № 1. С. 2–6.

совую связь и видеосвязь через Интернет между компьютерами, так и соответствующие платные услуги для звонков на мобильные и стационарные телефоны.

В правовом смысле программное обеспечение «Skype» – это программа, распространяемая компанией «Skype» Software S.a.r.l., обеспечивающая: а) бесплатную возможность соединения пользователей «Skype» через сеть передачи данных при оказании телематических услуг с целью передачи голосовой информации; б) платные услуги по установлению соединений между пользователями телефонной сети общего пользования и сети передачи данных «SkypeIN» и, наоборот, «SkypeOUT» с целью передачи голосовой информации[1].

Из-за отсутствия прямого указания в законе оснований, условий и порядка дистанционного получения показаний следователем или дознавателем появляются практические сложности: как надлежаще произвести допрос с использованием программы «Skype»?

Обращаясь по аналогии к положениям ст. 278.1 УПК РФ, отметим, что следователь или дознаватель, в чьем производстве находится уголовное дело и решивший дистанционно допросить свидетеля или потерпевшего, должен удостовериться в том, что программа «Skype» установлена на рабочем месте пользователя (свидетеля или потерпевшего), который имеет актуальные имя, логин или адрес электронной почты для входа. Об этом свидетель или потерпевший заранее извещает следователя или дознавателя заказным почтовым отправлением с уведомлением о вручении либо факсом, которое приобщается к материалам уголовного дела.

После этого следователь или дознаватель в соответствии со ст. 188 УПК извещает свидетеля или потерпевшего повесткой или посредством СМС-сообщения о дате и времени производства допроса не менее чем за 5 суток до его начала.

В назначенное время и дату должностное лицо, осуществляющее предварительное расследование по уголовному делу, с использованием персонального компьютера и сети Интернет осуществляет вход с помощью доступного ему логина или адреса электронной почты учетной записи «Майкрософт», а также пароля в программу «Skype», где в разделе «Поиск» вводит ставшее ему ранее известное имя, логин или адрес электронной почты пользователя (свидетеля или потерпевшего). Далее в результатах поиска выбирается необходимый профиль, после чего устанавливается видео-конференц-

[1] *Вайпан В.А.* Правовой режим оказания услуг связи Skype на территории Российской Федерации // Право и экономика. 2012. № 4. С. 48.

связь. Затем, до начала допроса, следователь (дознаватель) по месту нахождения свидетеля (потерпевшего) удостоверяется в личности последнего, разъясняет ему порядок производства следственного действия, права, обязанности и ответственность, после чего задает вопросы, относящиеся к предмету допроса.

По окончании допроса следователь (дознаватель) составляет протокол в порядке ст. 166 УПК РФ, в котором указываются технические средства, примененные при производстве следственного действия (ч. 5 ст. 190 УПК РФ) – персональный компьютер, программа «Skype» с именами, логинами или адресами электронной почты допрашивающего и допрашиваемого. Далее в протоколе следует отразить, что видеозапись допроса производилась с использованием MP3 Skype Recorder 4.43 на одноразовый оптический диск или иной электронный носитель информации, который по окончании следственного действия помещается в бумажный конверт, опечатывается и хранится при уголовном деле (ч. 4 ст. 189 УПК РФ).

Ввиду невозможности подписания допрашиваемым лицом протокола следственного действия в него вносится соответствующая запись, которая удостоверяется подписями следователя (дознавателя), понятых, а также представителя свидетеля или потерпевшего (ст. 167 УПК РФ).

Сказанное, тем не менее, не означает, что УПК РФ не нуждается в дополнении. Напротив, для устранения всяких сомнений с точки зрения допустимости данного доказательства необходимо как можно скорее прямо предусмотреть в законе право следователя (дознавателя) производить дистанционный допрос, который позволит сократить время и повысить эффективность досудебного производства по уголовным делам. При этом за основу могут быть взяты уже упомянутые нами положения ст. 278.1 УПК РФ, устанавливающие в самом общем виде особенности допроса свидетеля путем использования систем видео-конференц-связи в ходе судебного следствия.

Криптовалюты как предмет преступного посягательства в криминалистике

И. Г. Мухин,
врио начальника кафедры,
кандидат юридических наук
(Академия МВД Республики Беларусь)

В статье рассматриваются проблемы современной криминалистики, связанные с появлением и внедрением в экономику Беларуси нового вида нематериальных активов – криптовалют.

Криптовалюта, транзакция, цифровая валюта, цифровые токены, скрытый майнинг.

Развитие современных информационных и компьютерных технологий отражается практически на всех сферах жизнедеятельности общества. Закономерно, что в возможностях применения технических новинок заинтересован и преступный мир. Так, относительно недавно преступники стали использовать электронные деньги (WebMoney, QIWI, EasyPay и др.) для расчетов между собой. Одновременно с этим электронные деньги стали выступать в качестве предмета преступного посягательства. В настоящее время мировое сообщество столкнулось с такими новыми явлениями, как технологии реестра блоков транзакций (блокчейн) и криптовалюты.

2009-й год принято считать датой рождения криптовалют. Именно в этом году Сатоши Накамото (до сих пор неизвестно – это псевдоним одного человека или группы людей) опубликовал протокол Bitcoin и произвел первую транзакцию. Технологии реестра блоков транзакций развивались до конца 2017 г., пока не произошел резкий скачек курса Bitcoin на международных биржах: примерно с 1 000 долларов США в начале года до 19 500 долларов США 16 декабря 2017 г.[1] Также в 2017 г. все чаще начали появляются новости о правонарушениях, связанных с криптовалютами[2].

В итоге, в докладе Европола «Оценка угроз организованной интернет-преступности» (InternetOrganizedCrimeThreatAssessme

[1] Average USD market price across major bitcoin exchanges [Электронный ресурс]. Режим доступа: URL: https://blockchain.info/ru/charts/market-price?timespan=1year (дата обращения: 18.04.2018).

[2] Криминальный биткоин [Электронный ресурс]. Режим доступа: URL: https://iz.ru/684876/ivan-petrov/kriminalnyi-bitkoin (дата обращения: 18.04.2018).

nt – IOCTA) за 2017 год подчеркивается, что такие криптовалюты, как Monero, Ethereum и Zcash все чаще используются преступниками в качестве платежного средства на черных рынках. В то же время самой популярной цифровой валютой все еще остается Bitcoin. Популярность криптовалют в преступном мире Европол связывает, прежде всего, с деятельностью виртуальных магазинов по торговле наркотиками в теневом сегменте глобальной сети (Darknet)[1]. В это же время первые преступления, связанные с криптовалютами, зарегистрированы и на территории Республики Беларусь[2]. В деятельности правоохранительных органов появилась новая проблема: считать ли незаконное изъятие криптовалют преступлением против собственности?

В Республике Беларусь с принятием Декрета Президента Республики Беларусь № 8 от 21 декабря 2017 г. «О развитии цифровой экономики» фактически официально разрешены и законодательно отрегулированы правовые и экономические отношения, связанные с оборотом криптовалют. В то же время, на наш взгляд, недостаточно четко выражена позиция в отношении того, являются ли криптовалюты (цифровые знаки (токены)) имуществом (правом на имущество), что является существенным для применения уголовного и уголовно-процессуального законодательства. Так, пунктом 3 Приложения 1 к Декрету «владелец цифрового знака (токена)» определен как субъект гражданского права, которому цифровой знак (токен) принадлежит на праве собственности или на ином вещном праве. Кроме того, в пункте 3.4 Декрета сказано, что «для целей бухгалтерского учета... токены признаются активами». Таким образом, исходя из смысла ч. 1 ст. 210 Гражданского кодекса Республики Беларусь («Собственнику принадлежат права владения, пользования и распоряжения своим имуществом») и считая, что под понятием «активы» подразумевается бухгалтерское отражение реального имущества[3], мы можем сделать вывод о том, что в отечественном праве криптовалюта признается имуществом.

При формировании криминалистической характеристики имущественных преступлений, связанных с криптовалютами, мы счи-

---

[1] Crosscuttingcrimefactors [Электронный ресурс] (дата обращения: 18.04.2018).

[2] У белоруса украли биткоин. За это может быть уголовное наказание [Электронный ресурс]. Режим доступа: URL: https://tech.onliner.by/2017/12/13/bitcoin-39 (дата обращения: 18.04.2018).

[3] О соотношении понятий «актив», «собственность», «имущество» в российском праве [Электронный ресурс]. Режим доступа: URL: https://cyberleninka.ru/article/v/o-sootnoshenii-ponyatiy-aktiv-sobstvennost-imuschestvo-v-rossiyskom-prave (дата обращения: 18.04.2018).

таем, что во главу угла следует ставить сами цифровые токены, то есть непосредственный предмет преступного посягательства будет являться основным, системообразующим элементом. Этот признак имеет важное значение для правильной квалификации совершенного преступления, определения размера похищенного. Здесь важно заметить, что сведения о характере и размере ущерба, причиненного преступлением, образуют содержание не элемента криминалистической характеристики, а уголовно-правовой или же рассматриваются в перечне обстоятельств, подлежащих доказыванию. Кроме того, в том случае, если непосредственным предметом преступного посягательства будут криптовалюты, способ их отчуждения будет единственным – перевод с одного электронного кошелька (wallet) на другой, вне зависимости от формы хищения. Здесь мы видим проблему в доказывании такого важного признака хищения, как «чужое имущество». Достаточно ли потерпевшей стороне предоставить следователю сведения о своем электронном кошельке и электронном кошельке правонарушителя? После чего следователь сам обнаружит искомую транзакцию в реестре блокчейн и зафиксирует полученную информацию в протоколе осмотра. На наш взгляд, данная проблема требует дальнейшей проработки, учитывая относительную обезличенность всех операций с использованием криптовалют.

Учитывая то, что криптовалюты могут выступать не только в качестве предмета преступного посягательства, но и в качестве средства совершения преступления, мы также можем спрогнозировать рост следующих видов преступлений, связанных с оборотом цифровых токенов (выделены на основе анализа информации об обороте криптовалют в мире, опыта работы правоохранительных органов стран – участников СНГ и по итогам работы онлайн-семинара «Преступления, связанные с использованием криптовалюты: международный опыт расследований», состоявшейся 26 января 2018 г.):

1. Р*азличного рода хищения, например, мошенничества, как «обычные», общеуголовные, так и инвестиционные*[1]. Кроме того, зарегистрирована деятельность вредоносных программ, позволяющих совершать хищения путем использования компьютерной техники с применением методов фишинга[2].

---

[1] Литовский стартап исчез с 6 миллионами долларов, оставив инвесторам одно слово [Электронный ресурс]. Режим доступа: URL: https://42.tut.by/578749 (дата обращения: 28.04.2018).

[2] CryptoShuffler: троян, тихо наворовавший биткойнов на $140 000 [Электронный ресурс]. Режим доступа: URL: https://www.kaspersky.ru/blog/cryptoshuffler-bitcoin-stealer/19112/ (дата обращения: 28.04.2018).

2. *Преступления, связанные с деятельностью бирж, вовлеченных в оборот криптовалют.* В первую очередь это организация dDos-атак, что уже не раз случалось с международными биржами[1].

3. *Взяточничество с использованием криптовалют в качестве предмета взятки, а также легализация («отмывание») средств, полученных преступным путем.* В данном случае блокчейн-технологии выступают как средство сокрытия преступления. Также мы считаем, что использование блокчейн-технологий может рассматриваться как способ сокрытия преступления по иным видам коррупционных преступлений, при условии доказывания схемы «фидуциарные деньги → криптовалюта → фидуциарные деньги». Например, перед передачей криптовалюты в качестве предмета взятки взяткодатель приобретает на бирже Bitcoin за доллары США; производит транзакцию в Bitcoin (переводит на виртуальный кошелек взяткополучателя); взяткополучатель реализует Bitcoin, переводя криптовалюту обратно в фидуциарные деньги.

4. Кроме того, существует такое негативное проявление, как скрытый майнинг, что, по нашему мнению, может быть квалифицировано как *разработка, использование либо распространение вредоносных программ.*

На эффективность борьбы с указанными проявлениями преступности, на наш взгляд, повлияют эффективное законодательство, регулирующее деятельность в рассматриваемой сфере, а также готовность правоохранительных органов противостоять рассмотренным выше преступным проявлениям. Также считаем возможным предусмотреть обязательную оценку инвестиционной привлекательности ICO-проекта с точки зрения инвестиционных рисков и страхование ICO инвесторов. Кроме того, в рамках переподготовки сотрудников правоохранительных органов необходимо, на наш взгляд, предусмотреть изучение учебных дисциплин о технологиях реестра блоков транзакций (блокчейн) и криптовалютах.

---

[1] 7 способов атаковать биткоин [Электронный ресурс]. Режим доступа: URL: https://chainnews.ru/2017/12/16/7-sposobov-atakovat-bitkoin/ (дата обращения: 28.04.2018).

Перспективы развития и востребованность фоноскопических, лингвистических и автороведческих экспертиз при раскрытии и расследовании киберпреступлений

Т. В. Назарова,
начальник отдела
(ЭКЦ МВД России)

А. В. Громова,
старший эксперт,
кандидат филологических наук
(ЭКЦ МВД России)

В статье освещаются перспективы применения специальных знаний в области фоноскопических, лингвистических и автороведческих экспертиз при раскрытии и расследовании преступлений, совершаемых дистанционно с использованием современных технических средств.

Киберпреступления, эксперт, фоноскопическая экспертиза, лингвистическая экспертиза, автороведческая экспертиза.

В Доктрине информационной безопасности Российской Федерации, утвержденной указом Президента РФ от 5 декабря 2016 г. № 646, указывается, что «реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры»[1]. В числе основных направлений обеспечения информационной безопасности Доктриной определено противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации. Распространение указанной информации осуществляется, в первую очередь, посредством различных текстов, реализованных в рам-

[1] Доктрина информационной безопасности Российской Федерации (утв. указом Президента РФ от 5 декабря 2016 г. № 646) // Рос. газ. 2016. 6 дек.

ках дистанционной коммуникации, для которой используются интернет-платформы, специализированные программы (мессенджеры, скайп, социальные сети и др).

Понятие «киберпреступление» включает широкий спектр противоправных действий, начиная от вирусных атак, мошенничеств, кражи персональной информации и заканчивая преступлениями, связанными с распространением наркотиков, склонением к самоубийству, вовлечением в экстремистскую, террористическую и иную антиобщественную деятельность, осуществлением развратных действий в отношении малолетних и др. По мнению ряда исследователей, киберпреступления охватывают всю сферу информационных технологий, к которой относят как преступления, совершаемые с использованием компьютеров, так и преступления, предметом которых являются компьютеры, компьютерные сети и хранящаяся в них информация[1]. При этом компьютерные преступления рассматриваются как разновидность киберпреступлений, посягающих на безопасное функционирование компьютеров, компьютерных сетей и обрабатываемые ими данные.

В условиях цифровизации преступности свою специфику имеют как «виртуальные следы» (см. подробнее, например, в работах Мещерякова В. А.[2], Осипенко А. Л.[3], Введенской О. Ю.[4]),оставляемые при дистанционном совершении преступлений, так и особенности их сокрытия. Такие следы традиционно исследуются специалистами в области информационных технологий, компьютерных экспертиз. Однако, как показывает практика, оказывается не менее востребованным исследование текстовой и голосовой информации, посредством которых может осуществляться взаимодействие преступника с жертвой, а также сообщников при подготовке (обсуждении, планировании) или онлайн-сопровождении преступлений. В зависимости от поставленных задач письменная и устная речь исследуются в рамках фоноскопических, лингвистических и автороведческих экспертиз, производство которых организовано в экспертно-кри-

---

[1] *Номоконов В. А., Тропинина Т.Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). 2012. С. 45–55.

[2] *Мещеряков В.А.* Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежск. гос. ун-т, 2001.

[3] *Осипенко А.Л.* Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск, 2009.

[4] *Введенская О.Ю.* Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 210.

миналистических подразделениях органов внутренних дел Российской Федерации.

В экспертном сопровождении раскрытия и расследования преступлений, совершаемых с использованием сети Интернет, занимает особое местолингвистическая экспертиза. Посредством применения лингвистических специальных знаний в текстах могут быть выявлены признаки, соотносимые с такими преступлениями, как склонение, вербовка или иное вовлечение лица в деятельность экстремистского сообщества, склонение к совершению самоубийства; публичные призывы к осуществлению террористической деятельности или оправдание терроризма; развратные действия; возбуждение ненависти либо вражды; вымогательство; угроза убийством или причинением тяжкого вреда; незаконный оборот наркотических средств и др. Кроме того, может быть решена задача определения ролей и функций участников преступных групп посредством анализа их переписок или фонограмм разговоров.

В рамках фоноскопических экспертиз решаются задачи идентификации лиц по фонограммам речи и технического исследования фонограмм на предмет выявления признаков внесенных изменений. Возможность осуществления звуко – и видеозаписи любым обладателям смартфона, а также ее редактирования, моментального размещения и отправки любым пользователям создали предпосылки для случаев фиксации записей, на которых отражено как событие преступления (например, избиение несовершеннолетних, изнасилование, жестокое обращение с животными и др.), так и сведения о частной жизни лица, составляющие его личную, семейную тайну, а также какая-либо информация дискредитирующего характера. Для приобщения таких фонограмм к материалам дела, как правило, проводится фоноскопическая экспертиза с решением вопроса о наличии/отсутствии признаков неситуационных изменений зафиксированной на ней информации, исключения применения средств синтеза речи. При необходимости идентификации лиц, речь которых имеется на фонограммах, у подозреваемых изымаются образцы голоса и речи для проведения сравнительных исследований.

С учетом распространенности мессенджеров для осуществления коммуникации в настоящее время актуальной является задача исследования переписок, в ходе которых пользователи обмениваются как текстовыми, так и голосовыми сообщениями. Существуют определенные трудности при исследовании такого контента, однако при проведении комплексного исследования с привлечением специалистов в области фоноскопической и автороведческой экспертиз эта задача экспертами решается успешно.

Автороведческая экспертиза в последнее десятилетие претерпела существенные изменения, обусловленные характером объектов, к которым оказались неприменимы имеющиеся методические разработки – создание авторами текстов с использованием современных технических средств в условиях возможности мобильного обмена информацией. К настоящему времени разработаны и внедрены в практическую деятельность современные методики по автороведческой экспертизе, учитывающие актуальные достижения науки и техники в данной сфере и позволяющие решать задачи идентификации и диагностики лиц по текстам, создаваемым с использованием различных технических средств.

Поскольку современные технические возможности сокрытия IP-адресов и иных данных, позволяющих установить пользователя, активно используются злоумышленниками, идентификация лиц по оставленной ими текстовой информации представляется перспективным направлением экспертного сопровождения раскрытия и расследования преступлений. Как показывает практика, путем переписок непосредственно совершаются или подготавливаются преступления. Так, проведение автороведческих экспертиз может быть актуальным при доказывании факта участия конкретных лиц в переписке, связанной, например, с обсуждением дачи/получения взятки, с незаконным оборотом наркотических средств, с совершением мошенничеств в банковской сфере, вовлечением несовершеннолетних в так называемые группы смерти, совершением экстремистских преступлений, склонением их к участию в несогласованных митингах, акциях и иной незаконной деятельности.

Кроме того, важной областью применения средств и методов автороведческой экспертизы является возможность анализа текстов, озвученных с использованием средств синтеза речи или обладающих признаками интеллектуальной маскировки, когда инструментарий фоноскопической экспертизы не применим для идентификации лиц по голосу и речи. Данные ситуации актуальны, например, при вымогательстве, шантаже, похищении детей, угрозах, совершении мошенничеств и др.

С учетом реализации с 1 июля 2018 г. положений по пакету Яровой в части, касающейся хранения на территории Российской Федерации операторами связи и организаторами распространения информации в сети Интернет до шести месяцев текстовых сообщений и голосовой информации каждого из пользователей, у правоохранительных органов появляются колоссальные воз-

можности использования данной информации в случаях необходимости выявления, раскрытия и расследования преступлений. При этом прогнозируется рост востребованности в проведении лингвистических, автороведческих и фоноскопических экспертиз и исследований, которые могут быть эффективно задействованы в рамках экспертного сопровождения оперативных и следственных мероприятий по раскрытию и расследованию киберпреступлений, а также при реализации мер по противодействию угрозам национальной безопасности, защите несовершеннолетних от интернет-угроз.

Использование информационно-телекоммуникационных технологий в расследовании экологических преступлений

О. А. Петрухина,
доцент кафедры,
кандидат юридических наук
(Тульский государственный университет)

В статье обозначены перспективные направления использования информационно-телекоммуникационных технологий в расследовании экологических преступлений.

Информационно-телекоммуникационные технологии, экологические преступления, расследование преступлений.

В современных условиях развития криминалистической науки и техники информационно-телекоммуникационное обеспечение процесса расследования преступлений признается прогрессивным направлением, ему придается огромное значение[1].

Применительно к расследованию экологических преступлений оно является особо значимым, так как одной из основных особенностей данного процесса является объем и сложность получения информации о преступлении: ее отыскание, фиксация, изъятие, сохранение, анализ, оценка и использование. Это позволяет утверждать, что результативность их расследования имеет прямую зависимость от соответствующим образом организованной и эффективно функционирующей системы ее информационно-телекоммуникационного обеспечения.

С учетом специфики расследования преступных посягательств на объекты окружающей природной среды и современных возможностей информационных, телекоммуникационных средств и техно-

[1] Приказом Следственного комитета РФ от 15 января 2011 г. № 2 «Об организации предварительного расследования в Следственном комитете Российской Федерации» в целях установления единообразного порядка организации предварительного расследования в Следственном комитете РФ предписана необходимость организовать использование следователями современных компьютерных учетных и аналитических программ, в том числе специальных программно-технических комплексов («АРМ следователя»), вносить предложения по их совершенствованию, а также обеспечить доступ следователей по месту производства расследования к автоматизированным криминалистическим учетам, информационно-правовым системам, базам данных и сети Интернет (п. 1. 32).

логий мы в данной статье обозначили наиболее перспективные (на наш взгляд) направления их использования.

1. Объединение массивов криминалистически значимой для расследования экологических преступлений информации, сосредоточенной в различных автоматизированных информационно-поисковых системах, банках данных, в единую интегрированную автоматизированную информационно-поисковую систему – АИПС «Экология».

Создание и внедрение такой системы послужит важным фактором в повышении уровня организации взаимодействия дознавателя, следователя с сотрудниками иных служб правоохранительных органов и других ведомств.

Как известно, большая часть экологической информации аккумулируется в составе государственных информационных ресурсов. Взаимодействие предполагает взаимный обмен информацией, предоставление ее по запросам, передачу копий электронных баз данных, проведение совместных мероприятий. Однако такое взаимодействие осложняется узковедомственными интересами, что неприемлемо для полноценного расследования экологических преступлений.

Между тем, потребности практики их расследования настоятельно требуют системного подхода к организации межведомственного «электронного взаимодействия». К созданию единого предметно ориентированного информационного поля, в котором был бы возможен доступ в реальном времени к информационном базам данных (при условии соблюдения режима доступа), помимо органов, занимающихся расследованием экологических преступлений, нужно привлекать и такие органы, как: природоохранная прокуратура, Министерство природных ресурсов и экологии РФ, Департамент государственной политики и регулирования в сфере охраны окружающей среды, Департамент государственной политики и регулирования в области геологии и недропользования.

Выражением полномасштабного информационного поля должна стать интегрированная автоматизированная система, предоставляющая возможности оперативного обмена информацией между вышеуказанными органами, включающая базу криминалистически значимых данных о: лицах, ранее совершавших экологические преступления и правонарушения; предприятиях, нарушающих требования экологической безопасности; правилах ведения работ; видах и свойствах загрязняющих и отравляющих веществ и др.

При создании такой системы необходимо:

– учитывать разработки ученых-криминалистов, в частности криминалистические характеристики различных видов преступных нарушений природоохранных правил;

– использовать материалы уголовных дел, например обвинительные заключения (акты), которые будут направляться в автоматизированную систему для последующего анализа, с вычленением криминалистически значимых признаков и построением их возможных корреляционных связей.

Обязательным условием функционирования АИПС «Экология» должно быть своевременное и регулярное обновление криминалистически важной информации.

2. Внедрение мобильного автоматизированного рабочего места дознавателя, следователя (МАРМ (Д,С)). Использование данного программного продукта, сформированного на основе кибернетической модели процесса расследования, способно в несколько раз повысить технологичность и обеспеченность информацией в течение всей следственной деятельности, начиная от предварительного этапа и до окончания предварительного расследования[1].

Важность и актуальность внедрения и использования в деятельности по расследованию экологических преступлений именно *мобильного* АРМ (Д,С) обусловлена тем, что следственно-оперативной группе, следственной группе в ходе расследования большинства преступных посягательств на окружающую природную среду приходится выезжать на место происшествия, находящееся в десятках километров от постоянного места работы. Мобильное АРМ (Д,С), являясь переносным элементом стационарного автоматизированного рабочего места, позволит решить широкий круг задач, возлагаемых на стационарные АРМ дознавателя, следователя, а также получить оперативный доступ к требуемым базам данных.

Специальное программное обеспечение мобильного АРМ (Д,С), используемого при расследовании экологических преступлений, необходимо определять исходя из:

– типичных следственных ситуаций, складывающихся при расследовании разных классификационных групп экологических преступлений;

– содержательного описания следственных и процессуальных действий, выполняемых участниками следственно-оперативной группы, следственной группы при расследовании данных преступлений;

– разработанных и внедренных информационных моделей преступных посягательств на объекты окружающей природной среды.

---

[1] *Шурухнов Н.Г.* Назначение и роль автоматизированной системы органов предварительного следствия в расследовании преступлений // Уголовное судопроизводство: проблемы теории, нормотворчества и правоприменения: сборник научных трудов. Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2008. Вып. 3. С. 208.

Например, расследование фактов, связанных с загрязнением (отравлением) природной среды предполагает выполнение комплекса следственных и процессуальных действий, в числе которых первое место занимает осмотр места происшествия. Использование мобильного АРМ (Д,С) позволит дознавателю, следователю, находящемуся на предприятии – предполагаемом источнике загрязнения, правильно выбрать тактические приемы осмотра места происшествия, произвести сбор необходимых образцов для сравнительного исследования, использовать технические средства обнаружения, фиксации и изъятия вещественных доказательств, зафиксировать ход и результаты данного следственного действия, а также не забыть соблюсти все необходимые процессуальные требования.

Специальное программное обеспечение мобильного АРМ, используемого при расследовании преступных посягательств на экологическую безопасность, должно включать следующие компоненты:

1) средства доступа к нормативно-правовым базам, содержащим акты, регламентирующие сферу охраны окружающей среды;

2) средства доступа к информационным ресурсам, содержащим сведения о предприятиях – потенциальных загрязнителях; видах и свойствах загрязняющих и отравляющих веществ; лицах; холодном и огнестрельном оружии; паспортах и других объектах;

3) средства доступа к ресурсам федерального уровня – банку бланков процессуальных документов (постановление о возбуждении уголовного дела и принятии его к своему производству, постановления о производстве выемки, обыска, протоколы следственных действий, обвинительные заключения, акты, постановления);

4) справочные, экспертно-консультационные системы, например, содержащие алгоритмы действий (следственных, процессуальных, розыскных) в условиях наиболее распространенных следственных ситуаций, комплексы тактических и технологических приемов проведения различных следственных действий, ссылки на необходимые акты и инструкции;

5) программу оформления запросов, поручений, актов, сообщений;

6) программу обучения и контроля знаний, умений и навыков дознавателей, следователей.

Использование МАРМ (Д,С) перспективно при проведении практически любого следственного, процессуального, организационного действия. Возможности мобильного АРМ, применяемые в расследовании экологических преступлений, определяются программным обеспечением, объемом и содержанием баз

данных. Широкие перспективы открывает использование различных компьютерных технологий, которые могут применяться для статистической обработки данных, создания специализированных информационно-поисковых систем с соответствующими базами данных.

3. Внедрение информационно-телекоммуникационных технологий в экспертную деятельность.

Опрашиваемые нами судебные эксперты-экологи на вопрос о процессуальных и тактических отличиях производства судебно-экологических экспертиз в Российской Федерации и в зарубежных государствах назвали использование зарубежными экспертами-экологами математической обработки компьютерами результатов экспертного исследования. Указав при этом, что применение такой программы значительно повышает качество судебно-экологической экспертной деятельности.

К сожалению, в российской науке данному перспективному направлению уделяется очень мало внимания, что непосредственно сказывается на эффективности производства судебно-экологических экспертиз.

Применение компьютерных информационных технологий в судебно-экологической экспертизе должно быть направлено на разработку программных комплексов автоматизированного решения экспертных задач, включающих не только компьютеризацию трудоемких расчетов, но и программные модули, используемые для составления экспертных заключений[1]. Данные модули можно наполнить конкретным содержанием в зависимости от используемой при производстве определенного вида исследования экспертной методики. Это позволит избежать совершения экспертных ошибок субъективного характера и сократить время, необходимое для подготовки экспертного заключения. Экономия времени особенно важна, так как, проанализировав практику расследования преступных посягательств на объекты окружающей природной среды и опросив практических работников, мы пришли к выводу, что одним из основных факторов, сдерживающих быстрое и эффективное расследование данных преступлений, является длительность сроков производства судебно-экологиче-

[1] См. об этом: *Толстухина Т.В.* Современные тенденции развития судебной экспертизы на основе информационных технологий: дис. ... д-ра юрид. наук. М., 1999. 320 с.; *Россинская Е.Р.* Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. М., 2006. 256 с.; *Сретенцев Д.Н.* Основные направления информационно-аналитического обеспечения судебно-экспертной деятельности: учебное пособие. Орел, 2008. С. 23.

ских экспертиз. Таким образом, актуальность и востребованность развития и внедрения информационно-телекоммуникационных технологий в деятельность по расследованию экологических преступлений являются очевидными. Огромный арсенал средств и методов информационных, телекоммуникационных систем представляет широчайшие дополнительные возможности для эффективного расследования данных преступлений, а их дальнейшее развитие служит основой специальных исследований, носящих перспективный характер.

Уголовно-процессуальное законодательство Российской Федерации: оцифровать или одухотворить?

А. В. Победкин,
профессор кафедры,
доктор юридических наук, профессор
(Академия управления МВД России)

В статье рассматривается вопрос о необходимости отражения в уголовно-процессуальном законодательстве России особенностей использования цифровых технологий. Делается вывод о том, что решение иных проблем уголовного судопроизводства в настоящее время является более актуальной задачей.

Процессуальная форма, цифровые технологии, нравственные начала уголовно-процессуальной деятельности.

Нет никаких сомнений в том, что развитие цифровых технологий существенно влияет на все сферы человеческой жизни, фактически создает новую «цифровую реальность»[1]. Цифровые технологии не только позволяют более удобно и комфортно жить, но и мощно влияют на самого человека, а через него – на все общество. Цифровизация исподволь «переделывает» человека, «переплавляет» его. Будем честны, эта «переплавка» весьма опасна механизацией человека, его духовной примитивизацией, снижением интеллектуально-поисковой активности. «Цифровая реальность» требует «противовеса», «антидота», нейтрализующего ее негативное воздействие на духовно-интеллектуальную сферу человека.

История показала, что создать «нового», в духовном смысле, человека не удалось за тысячелетия. Он по-прежнему руководствуется биологическими инстинктами и в нравственном смысле только в начале пути к Человеку, в котором преобладает духовное.

Надежды на такое преобразование возлагались на революционные события, столетие которых Россия отметила менее года назад. Многие верили в возможность рождения другого человека из гущи величайших социальных потрясений, скорых и жестоких. Пришлось разочароваться. Социальные потрясения не только не способны в одночасье перелицевать человека в Человека, но и откры-

[1] *Зорькин В. Д.* Право в цифровом мире // Рос. газ. 2018. 30 мая.

вают «шлюз» инстинктам животного толка, которые нередко становятся руководящим началом, единственной мотивацией к действию. «Мы, батюшка, не можем себе волю дать. Взять хоть меня такого-то. Ты не смотри, что я такой смирный. Я хорош и добер, пока мне воли не дашь. А то первым разбойником, первым грабителем, первым вором. Первым пьяницей окажусь...», – заметил И. А. Бунину «один орловский мужик»[1].

Ясно, что нравственные качества достойные Человека не могут взяться из ничего, из одного только стремления разрушить Зло. На его разрухах всегда стремится разрастись Зло новое. Человеческие качества (не человеческие, а Человеческие) рождаются, приживаются и приобретают силу в человеке только в результате непрерывной, нескончаемой, тяжелой воспитательной работы. Нравственность – истончаемая и хрупкая ценность, которая слетает с человека, как осенние листья с дерева даже при легком порыве ветра. Так случилось в России в конце прошлого века. Будто бы и не было 70-летней истории создания нового Человека, действительно проникнутой стремлением взрастить духовную, а не животную личность. Оправляться придется еще долго.

Цифровизация мира – не революция и не эпоха, как вряд ли верно считать революциями и эпохами пользование лошадьми, телегами, автомобилями, даже космическими кораблями. В конечном итоге – это только утилитарные средства, продукт эволюции, который, между тем, способен поработить и изуродовать Человека, если он не определит им место в системе социальных ценностей.

Не будем преуменьшать ни значения, ни опасности цифровых технологий. Они, несомненно, прорывные, однако сотворение из них Культа, Божества, требующего в жертву всего Человека, забирающего все его мысли, чувства, стремления, интересы неизбежно запускает обратный процесс: превращения Человека (которого еще создавать и создавать) в человека. Только в сочетании с воспитанием нравственности, усиливающимся по мере развития цифровых технологий, цифровизация принесет пользу.

Поэтому наряду со Стратегией развития информационного общества в Российской Федерации на 2017–2013 годы[2] реализу-

---

[1] *Бунин И.А.* Окаянные дни: дневники, статьи, воспоминания / Иван Бунин. М.: Эксмо, 2011. С. 493.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901.

ется и Стратегия развития воспитания в Российской Федерации на период до 2025 года[1].

Пока же Божество цифровизации стремиться поглотить и преклонить всю жизнь общества. Право – тоже на пути развивающейся цифровизации. В. Д. Зорькин пишет, что право в этих обстоятельствах нуждается в существенной модернизации: подобно «тому, как правила дорожного движения, рассчитанные на регулирование езды на лошадях, сменились правилами автомобильного движения, правилами авиаперевозок и космических полетов, так и сегодня зарождается новое право – «право второго модерна», регулирующее экономические, политические и социальные отношения в контексте мира цифр, больших данных, роботов, искусственного интеллекта»[2].

Да, право должно развиваться, регулировать новые общественные отношения, соответствовать уровню развития общества. Однако к его совершенствованию необходим дифференцированный подход. Новые общественные отношения требуют существенной модернизации только тех отраслей права, которые предназначены для их регулирования, а не всех подряд.

Аппетиты цифровизации ныне достигли и уголовного судопроизводства. Ширится спектр научных исследований, результатом которых становятся выводы либо о необходимости отражения в уголовно-процессуальном законодательстве всех тонкостей работы с цифровыми технологиями, либо сводящиеся к предложению лозунговых новелл, попросту напоминающих, что Божество в виде «цифры» существует. Вот уж поистине и то и другое создание «сущности без нужды».

Спора нет, отдельные особенности работы с расширяющимся сегментом электронных носителей информации в уголовно-процессуальном законодательстве предусмотреть необходимо. Вероятно, это касается некоторых правил их изъятия, копирования, описания в протоколах, хранения. Нужно ясно разграничить виды доказательств, которые могут быть сформированы на основе таких носителей, поскольку сегодня они и законодателем, и правоприменителем рассматриваются только как вещественные доказательства, хотя нередко фактически являются иными документами. Неплохо бы предусмотреть особенности копирования электронной информации и ее осмотра.

---

[1] Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 г.: распоряжение Правительства РФ от 29 мая 2015 г. № 996-р // Собр. законодательства Рос. Федерации. 2015. № 23. Ст. 3357.

[2] *Зорькин В. Д.* Право в цифровом мире // Рос. газ. 2018. 30 мая.

В. Д. Зорькин, называющий право в условиях развития информационного общества «правом второго модерна» и отмечающий, что специалисты прогнозируют революцию в познавательно-доказательственной базе, называет в числе ее признаков только появление цифровых следов как электронных доказательств, новых видов судебных экспертиз и систем электронного участия в процессе[1]. Остальные признаки – за рамками уголовного процесса, они делопроизводственные и носят организационный характер. Полагаем, говорить о революции в доказывании на основании приведенных признаков нельзя.

В целом все нужные правила для эффективного использования информации, содержащейся на электронных носителях, в Уголовно-процессуальном кодексе Российской Федерации (далее – УПК) уже предусмотрены и по большому счету их вполне достаточно.

Вряд ли в игнорировании информационных технологий можно упрекнуть государства, которые принято считать развитыми в технологической сфере, например ФРГ, Францию и др. Между тем, уголовно-процессуальное законодательство этих стран выдержано вполне в «гуманитарном» содержании.

Так, в Уголовно-процессуальном кодексе Франции из числа средств, которые напрямую не известны отечественному законодательству, предусмотрен порядок перехвата сообщений, передаваемых с помощью средств телекоммуникации, по решению следственного судьи силами любого компетентного должностного лица, в ведении которого находятся каналы связи. Уголовно-процессуальный кодекс Федеративной Республики Германии не различает процессуальные и оперативно-розыскные мероприятия в отечественном понимании и только потому в нем нашел отражение несколько более широкий спектр действий с использованием информационных технологий: контроль телекоммуникации, который может применяться в отношении телекоммуникации любого вида, в том числе при передаче информации, сгенерированной компьютером, на компьютере, передаваемой посредством сети Интернет и по факсу; прослушивание и запись высказываний, сделанных непублично; тайная фото-, кино-, видеосъемка; компьютерный поиск (автоматические сравнение личных данных с имеющейся информацией).

Не ушли вперед и государства постсоветского пространства. В Грузии, где тайные следственные действия являются процессуальными средствами, позволено контролировать данные интернет-трафика, снимать информацию с технических каналов связи.

[1] *Зорькин В. Д.* Право в цифровом мире // Рос. газ. 2018. 30 мая.

В Уголовно-процессуальном законодательстве Эстонии достаточно детально регламентирован порядок хранения, передачи, уничтожения компьютерных файлов.

Собственно, ничего революционного. Не будем отрицать, что потребность во внедрении информационных цифровых технологий в работу должностных лиц, осуществляющих уголовное судопроизводство, существует, но для этого не нужно наполнять УПК организационно-делопроизводственными правилами электронного документооборота.

В уголовно-процессуальном законодательстве России сегодня острый дефицит не «цифровых» процедур, а одухотворяющих, воспитывающих правил. Они, необходимые в любом уголовно-процессуальном законодательстве, в современном российском оказались донельзя выхолощенными, а многочисленные предложения оцифровать уголовный процесс вплоть до отказа от процессуальной формы тем более выводят одухотворение уголовно-процессуального права в число первоочередных задач.

Прежде всего уголовный процесс нельзя строить на чужеродных для России и в принципе безнравственных идеях «сделок», «удешевлений», «медиаций» и прочих суррогатов уголовно-процессуального доказывания, губящих высокий нравственный смысл деятельности по установлению лица действительно виновного в совершении преступления и назначении ему справедливого наказания. Ответственность за ее результаты следователь, дознаватель, прокурор, судья несут не перед руководителями, не перед профессиональным сообществом, не перед участниками процесса, а перед обществом и каждым его членом. Публичность уголовного процесса особо значима в России, сила которой всегда определялась «миром», «коллективом», в отличие от западного индивидуализма.

Пусть невольно, но приоритет коллектива перед правами и свободами конкретного человека заложен и в Конституции Российской Федерации (далее – Конституция), которая, предусматривая их в качестве высшей ценности, позволяет ограничивать ради основ конституционного строя, нравственности, здоровья, прав и свобод других лиц, обороны страны и безопасности государства (ч. 3 ст. 55 Конституции).

Остается только согласиться с авторами проекта Концепции уголовной политики, разработанной Центром стратегических разработок совместно с Советом Федерации, что чужеродные англосаксонские идеи не приносят пользу отечественному судопроизводству.

Только при соответствии «уголовно-процессуального права культурно-историческому и духовно-нравственному наследию нашего народа» оно способно оказать «положительное влияние на духовную жизнь российской общности и формирование ее культуры»[1].

В целях развития одухотворяющих начал уголовного судопроизводства необходимо отойти от технократичного отношения к основным положениям УПК, которым посвящен его Раздел I. Именно здесь место идеям и требованиям, заключающим в себя «дух закона», который, кроме одухотворяющего и воспитательного значения, имеет вполне конкретное содержание и значение как основа юридических приемов толкования норм права и применения аналогии. Стоит ли говорить, что не «одухотворенные» общие положения уголовно-процессуального законодательства – основная причина ничтожного воспитательного заряда УПК.

«Основные положения» УПК на сегодня – эклектичный набор норм, значительная часть которых по содержанию не может считаться основными положениями уголовно-процессуального права. Претендовать на такую роль не могут основания отказа в возбуждении уголовного дела, прекращения уголовного дела и уголовного преследования (гл. 4 УПК). Глава 3 УПК, посвященная правилам осуществления уголовного преследования, изложена в редакции, маскирующей публичность как основную функцию уголовного судопроизводства. Эта глава в ее современном виде – банальные регулятивные нормы.

В числе общих положений УПК не нашлось места норме, из содержания которой можно получить внятное представление о методе уголовно-процессуального регулирования, основной признак которого, на наш взгляд, – обязанность должностных лиц предпринимать все возможные законные меры к удовлетворению публичного интереса в исходе уголовного судопроизводства, невозможность диспозитивного поведения, действий по усмотрению.

В связи с этим в разделе I УПК важно предусмотреть, что уголовный процесс имеет основной функцией, предназначением – публичность, т. е. обеспечивает безопасность общества от преступлений путем правильного установления обстоятельств по уголовному делу, что позволяет привлекать к уголовной

[1] *Агутин А. В., Трошкин Е. З., Губжоков Р. Х.* Организационно-правовой механизм реализации концепции «должной правовой процедуры» и нравственные основы уголовно-процессуальной деятельности в отечественном уголовном судопроизводстве». М.: Юрлитинформ, 2016. С. 149.

ответственности и осуждать только тех, кто в действительности совершил преступление.

Слабость Раздела I УПК и в том, что в нем умалчивается о целях и задачах уголовного судопроизводства. К чему плодить дискуссии относительно содержания понятия назначения уголовного судопроизводства, пытаясь усмотреть в нем некие цели и задачи. Их там нет. Назначение, цели и задачи –понятия непересекающиеся, а правильно сориентированные, правоприменитель и законодатель действуют не в пример эффективнее дезориентированных.

Глубинной реформе необходимо подвергнуть гл. 2 УПК, закрепляющую систему принципов уголовного судопроизводства. Сегодня они не выполняют функцию основных, концептуальных идей, пронизывающих уголовное судопроизводство, ориентирующих законодателя и правоприменителя, и если не будут модернизированы по форме и содержанию, указанную главу вполне безболезненно можно исключить из закона. Вряд ли имеются основания всерьез отрицать, что современное уголовное судопроизводство России не укладывается в принцип презумпции невиновности, свободы оценки доказательств, уважения чести и достоинства личности, законности, равенства всех перед законом и судом. Свидетельство тому – продолжающееся расширение оснований прекращения уголовного дела по нереабилитирующим основаниям, назначение уголовных квазинаказаний без полноценной судебной процедуры, признание виновным фактически на основании признания обвиняемым вины, отказ от полноценного процесса доказывания в сокращенных досудебных процедурах, раздутые иммунитеты.

Принципы должны быть внятными идеями концептуального характера, близкими и понятными каждому жителю страны, одухотворяющими закон и человека, его применяющего. В связи с этим попытки заложить в статью, посвященную принципу, его исчерпывающее содержание, к тому же нормами банального регулятивного характера, – непродуктивно.

Систему принципов нужно очистить от регулятивных уголовно-процессуальных норм, или субъективных прав, свобод и обязанностей участников судопроизводства, тем более, что некоторые из них дублируют конституционные положения. Идеи первичны относительно прав, свобод и обязанностей, являются для них основой и определяют пределы.

В числе одухотворяющих идей нужно найти место таким, как совесть, служение, гуманизм, милосердие, справедливость, честность, долг, истина. «Ментальная модель истины-правды в отечественном уголовном судопроизводстве окроплена многовековой

мудростью нашего народа. Ментальная модель истины-правды подобна верным знаниям местности, посредством которых мы ориентируемся в пространстве и времени. В этом смысле истина-правда образует в уголовно-процессуальной сфере те убеждения и верования, на которые мы ориентируемся в реалиях уголовного судопроизводства. Ментальная модель истины-правды имеется в каждом из нас»[1]. Значит, ей место и в УПК.

Дух закона должен быть неколебим, а для этого целесообразно рассмотреть вопрос об усложненном порядке внесения изменений и дополнений в раздел УПК, содержащий основные положения уголовного судопроизводства.

Цифровизация уголовного судопроизводства через цифровизацию уголовно-процессуального права – больше дань моде, чем объективная необходимость. В уголовно-процессуальном праве в целом есть все необходимые средства для эффективной работы с информацией любой физической формы. Оптимизация работы должностных лиц, отвечающих за конкретное уголовное судопроизводство, внедрение передовых технологий в их повседневную деятельность никаких возражений вызывать не может. Однако потрясать для этого уголовно-процессуальное право нет достаточных оснований. Уголовное судопроизводство нуждается сегодня не в цифровизации, а в одухотворении. «Что значат законы без нравов и веры?» – вопросил Гораций. Все, что нам нужно, великими уже сказано.

---

[1] *Агутин А. В., Трошкин Е. З., Губжоков Р. Х.* Организационно-правовой механизм реализации концепции «должной правовой процедуры» и нравственные основы уголовно-процессуальной деятельности в отечественном уголовном судопроизводстве». М.: Юрлитинформ, 2016. С. 182.

Особенности построения алгоритмов и информационно-методического обеспечения «перманентной» квалификации преступлений в сфере экономики

В. А. Прорвич,
доктор юридических наук, доктор технических наук, профессор (Московская академия Следственного комитета Российской Федерации)

В статье рассматриваются особенности алгоритмов формирования системы юридических тождеств для квалификации преступлений в сфере экономики на различных стадиях их выявления, раскрытия и расследования, включая использование положений гражданского и специального законодательства для раскрытия бланкетных диспозиций соответствующих уголовно-правовых норм.

Квалификация преступлений в сфере экономики, выявление, раскрытие, расследование преступлений, раскрытие бланкетных диспозиций.

Анализ правоприменительной практики показывает, что уголовно-правовая защита от преступлений в сфере экономики и финансов далека от совершенства и нуждается в комплексном укреплении на всех уровнях – от правотворчества до правоприменения, включая научно-методическое обеспечение деятельности правоохранительных органов и судов, в том числе с использованием современных информационных технологий. Актуальность соответствующих проблем резко возрастает и в связи с быстрым развитием новых секторов цифровой экономики, применением технологии «блокчейн», созданием на ее основе «крипловалют», а также созданием иных «суперсовременных» финансовых инструментов, не предусмотренных действующим законодательством.

Одной из давно назревших проблем научно-методического и информационного обеспечения работ по выявлению, раскрытию и расследованию преступлений рассматриваемого вида является их «перманентная» квалификация на всех этапах организации и выполнения соответствующих следственных действий. Это становится еще более актуальным с учетом бурного развития различных отраслей современной цифровой экономики, оперирующей нематериальными активами, представленными в виде групп определенных символов на электронных носителях с использованием специаль-

ных информационных технологий. Тем более, что процессы законотворчества в данной сфере общественных отношений существенно отстают от темпов роста криминальных проявлений в новых отраслях цифровой экономики. При этом латентность новых видов преступлений в сфере экономики не только возрастает, но и приобретает новый характер зашифрованных криминальных действий в виртуальном пространстве, для идентификации которых требуется взаимодействие со специалистами высшей квалификации.

Понятно, что первоначальные этапы постановки соответствующих научных исследований и разработок, охватывающих все этапы выявления, раскрытия и расследования преступлений в сфере «обычной» и цифровой экономики и нацеленных на создание современного информационно-методического обеспечения следственных и иных процессуальных действий, должны осуществляться ведущими учеными и специалистами в различных отраслях наук уголовно-правового цикла. Разнобой в подходах к созданию соответствующих алгоритмов и их практической реализации в виде «фирменных» компьютерных программ может привести к возникновению неприемлемо высоких уровней рисков выхода «информационщиков» за рамки уголовного права.

То есть речь идет о необходимости формирования научно обоснованной и выверенной практикой иерархической системы алгоритмов обработки информации, имеющей правовой статус, с обеспечением контроля за сохранением статуса всех промежуточных и итоговых результатов такой отработки. В этой иерархии алгоритмов должны найти свое место взаимосвязанные алгоритмы не только тех действий по преобразованию статусной информации, которые осуществляет сам следователь в рамках общей и частных криминалистических методик, но и иных процессуально регламентированных действий, предусматривающих взаимодействие следователя с иными участниками уголовного судопроизводства. Кроме того, необходимо вписать в эту иерархию и такие алгоритмы, которые связаны с применением специальных знаний судебных экспертов и специалистов в рамках соответствующих экспертных методик для получения доказательств по уголовным делам любой сложности на основе «виртуальных» следов особого характера.

Для выявления и фиксации рассеянных идеальных следов многих видов преступлений в сфере экономики, которые выявляются не по наличию, а по отсутствию в документах определенной информации, предусмотренной требованиями действующего законодательства, необходим специальный инструментарий. Его создание возможно только на основе применения современного информа-

ционного обеспечения с обширными базами данных и классификаторами сведений, имеющих правовой статус. По мере развития различных отраслей цифровой экономики и проникновения криминала в данную сферу необходимость в развитии и дальнейшем совершенствовании такого инструментария будет только возрастать.

В рамках подобных алгоритмов создается ряд возможностей и для профилактики юридических ошибок, связанных с попытками использования таких сведений о фактах, которые не прошли надлежащую проверку и оценку. Тем более, что правовой статус используемых сведений о фактах может не только связываться с источниками соответствующей информации, но и ранжироваться в соответствии с установленными требованиями. Фактически в систему разрабатываемых алгоритмов могут быть встроены также и критерии проверки и оценки доказательств, установленные уголовно-процессуальным законодательством.

При создании достаточно полной системы алгоритмов обработки информации, имеющей правовой статус, перед следователем, а затем прокурором и судьей уже не будут ставиться такие исследовательские задачи, решение которых под силу лишь крупным научным коллективам. Эти задачи как раз и будут решаться ведущими учеными в соответствующих областях наук, включая проблемы на стыке нескольких отраслей научного знания. А следователь, прокурор и судья будут оснащены современным инструментарием, разработанным научными коллективами, с помощью которого каждый из них сможет в кратчайшие сроки получить несколько вариантов выверенных решений, на основе которых сформирует свое собственное решение и сможет его надлежащим образом обосновать.

На этой основе в достаточно короткие сроки может быть сформирована и система обратных связей следователей, прокуроров и судей с ведущими учеными страны, обеспечивающая формирование нескольких групп проблемно-ориентированных совокупностей новых эмпирических фактов, отражающих сложившуюся ситуацию в уголовном судопроизводстве по преступлениям в сфере экономики. С их использованием возможно создать научно обоснованный базис для обобщения тех общественных процессов, которые позволят найти ответы на новые вызовы криминала.

Необходимо обратить внимание и на особенности тех логических конструкций, которые выстраиваются следователями при идентификации признаков преступления в соответствии с диспозицией определенной уголовно-правовой нормы. Как правило, они носят «линейный» характер, составляя цепочку определенных фак-

тов, связанных причинно-следственными связями, либо несколько разветвляющихся цепочек подобного вида. Но при идентификации сложных видов преступлений в сфере экономики требуется проанализировать существенно больше вариантов логических связей между различными субъектами финансово-хозяйственной деятельности в рамках системы обязательственных прав. Для этого часто оказывается необходимой формализация имеющихся сведений с помощью двумерных и многомерных матричных классификаторов, позволяющая наглядно представить систему правоотношений законопослушных экономических субъектов, на фоне которой можно обнаружить допущенные нарушения требований действующего законодательства субъектами конкретного преступления.

Создавая соответствующее методическое обеспечение, необходимо надлежащим образом формализовать характеристики субъектно-объектных и субъектно-субъектных отношений фигурантов различных видов преступлений в сфере экономики. Именно «многомерная» характеристика отношений законопослушных экономических субъектов различного вида и уровня позволяет наглядно представить характеристики того «правового поля», в рамках которого они обладают полной свободой предпринимательской и иной деятельности. При этом фактически речь идет о развернутой многомерной информационной характеристике важнейшего принципа автономии воли экономических субъектов, введенного и раскрытого в самых первых статьях Гражданского кодекса РФ с указанием на существующие законодательные ограничения.

Но при всей наглядности и современности такого информационного обеспечения возникает ряд проблем со словесным описанием хотя бы основных вариантов сочетаний тех правовых норм гражданского и специального законодательства, которым должен следовать законопослушный экономический субъект, взаимодействующий или просто имеющий какое-либо отношение к деятельности других экономических субъектов на этом правовом поле. Достаточно упомянуть лишь о том, что ежегодно принимается несколько тысяч нормативных правовых актов, которые существенно изменяют характеристики не только самого правового поля, но и варианты тех маршрутов, по которым могут двигаться в рамках своего бизнеса законопослушные экономические субъекты.

С использованием матричного подхода можно выявить не только основные особенности субъектно-объектных и субъектно-субъектных отношений фигурантов преступлений, связанных с определенными видами преступлений в сфере экономики, и формирования их «многомерной» уголовно-правовой характеристики. Комбини-

руя различные группы признаков преступлений, отражающих объект, объективную сторону, субъект и субъективную сторону расследуемого преступления в строках и столбцах нескольких матриц, возможно не только выявить такие группы признаков преступлений, которые далеко не всегда очевидны при обычном, «линейном» подходе к идентификации преступлений рассматриваемого вида. Важно обратить внимание на возможности «динамического» матричного анализа правоотношений экономических субъектов, позволяющего выявить особенности приготовления к совершению преступления, способы его совершения, а также использованные приемы для сокрытия его следов.

При этом с точки зрения надлежащего формирования юридического тождества, используемого для квалификации конкретного преступления, левая часть тождества, содержащая первичные сведения о преступлении и результаты их проверки, как правило, характеризуется «информационной недостаточностью». В то же время его правая часть, сформированная на основе признаков состава преступления, отличается «информационной избыточностью». То есть количество имеющихся в распоряжении следователя доказательств на стадии решения вопроса о необходимости возбуждения уголовного дела и обоснования соответствующего постановления всегда намного меньше общего количества признаков состава преступления, сформированных законодателем в соответствующих статьях УК РФ.

Первый вариант алгоритма следственных действий, которые приходится выполнять при решении вопроса о возбуждении уголовного дела и обоснования соответствующего постановления, характеризуется наибольшими неопределенностями в системе исходных данных для квалификации преступления и предполагает формирование и сопоставление нескольких вариантов юридического тождества. Они должны охватывать ряд «смежных» видов преступлений в сфере экономики.

Необходимо также учитывать, что специфической особенностью алгоритмов квалификации преступления на начальной стадии следственных действий является заложенный в них принцип дополнительности. Речь идет как о дополнении данного алгоритма планом следственных действий и оперативных мероприятий для получения недостающей информации, так и об использовании в рамках режима последовательных приближений дополнительного алгоритма, позволяющего более детально раскрыть бланкетные диспозиции одной или нескольких выбранных следователем для квалификации преступления уголовно-правовых норм.

На последующем этапе расследования преступления требуется применение несколько иного алгоритма квалификации преступления, позволяющего обеспечить весь комплекс следственных действий, нацеленных на проведение надлежащего расследования данного преступления. При этом алгоритм раскрытия бланкетной диспозиции соответствующей уголовно-правовой нормы на основе проблемно-ориентированного группирования правовых норм гражданского и иного специального законодательства наиболее целесообразно построить на основе метода последовательных приближений.

Проведенное рассмотрение позволяет сделать вывод о том, что на протяжении всего процесса расследования уголовного дела, связанного с определенным видом преступления в сфере экономики, фактически речь идет об информационно-методическом обеспечении «перманентной» квалификации преступления. При этом на каждом из этапов расследования производится не только постепенная детализация развернутой уголовно-правовой характеристики при раскрытии бланкетной диспозиции соответствующей уголовно-правовой нормы с применением все большего количества правовых норм гражданского и иного специального законодательства, но и более точная идентификация состава данного преступления. Следователь получает возможность проведения сравнительного исследования нескольких вариантов юридического тождества, в рамках которых собранная система доказательств сопоставляется с детализированными до необходимой степени бланкетными диспозициями нескольких уголовно-правовых норм и всеми признаками состава расследуемого преступления.

Следует подчеркнуть, что в рамках разработанной системы алгоритмов создается возможность проведения параметрического анализа отдельных составляющих системы юридических тождеств при сопоставлении собранной системы доказательств с отдельными составляющими уголовно-правовых норм. При использовании соответствующего информационного и методического обеспечения это позволяет выявить особенности объекта и предмета расследуемого вида мошенничества, а также его объективной стороны. По результатам такого анализа можно выявить и ряд признаков определенной совокупности преступлений в сфере экономики, совершенных одним лицом. Итоговый вариант алгоритма квалификации мошенничества определенного вида и сформированной для этого развернутой системы юридических тождеств может быть сориентирован на завершающую стадию следственных действий, связанных с подготовкой обвинительного заключения. Решить проблему установле-

ния достаточности собранной совокупности доказательств возможно на основе применения алгоритмов квалификации преступления, описанных выше, с применением развернутой системы юридических тождеств[1].

Естественно, что речь ни в коем случае не идет о том, чтобы полностью автоматизировать эту часть работы следователя и поручить ее компьютеру, оснащенному соответствующим программным обеспечением, базами данных и базами знаний. При практической реализации этих алгоритмов следует ориентироваться на создание интерактивных программно-аппаратных комплексов, обеспечивающих максимальное удобство диалога следователя с компьютером.

[1] Организация и методика расследования отдельных видов экономических преступлений / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: «Спутник+», 2016.

Особенности допроса свидетелей при расследовании киберпреступлений

Т. В. Радченко,
старший преподаватель кафедры,
кандидат юридических наук
(Московский университет МВД России
им. В. Я. Кикотя)

В статье рассматриваются основные аспекты организации и проведения допроса свидетелей при расследовании преступлений, совершаемых с применением IT-технологий. Обоснована необходимость привлечения специалиста на этапе подготовки к проведению допроса.

Специфические признаки киберпреступности, трудности расследования, допрос свидетелей.

Мировое сообщество рассматривает киберпреступность как глобальную международную проблему, о чем свидетельствуют принятые в последние годы международные договоренности, которые предусматривают совместные усилия по борьбе с этим высокотехнологичным злом. По мнению экспертов ООН, под киберпреступностью следует понимать любое противозаконное действие, совершаемое в виртуальном пространстве[1]. Опасность киберпреступности как для мирового сообщества в целом, так и для России является очевидной. Так, по данным Главного управления специальных технических мероприятий МВД России, киберпреступность в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере[2].

Преступления, совершаемые в этой сфере, обладают рядом специфических признаков:

– как правило, такие деяния имеют высокий уровень латентности: применение анонимайзеров либо выход в сеть через «подставные компьютеры» (например, в интернет-кафе) – все это делает практически невозможным установление личности преступника;

[1] Доклад Управления ООН по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности». 2013 // URL: http://pdf.knigi-x.ru/21yuridicheskie/136262-1-unp-oon-upravlenie-organizacii-obedinennih-naciy-narkotikam-prestupnosti-vsestoronnee-issle.php.

[2] URL: http://www.crime-research.ru/library/Mirosh1.html (дата обращения: 18.04.2018).

– для подобных преступных деяний свойственна так называемая трансграничность. Иными словами, преступник и его «жертва» могут находиться на любом удалении друг от друга;

– преступления совершаются, как правило, в автоматизированном режиме. Хакерами разработаны и «вполне успешно» (с точки зрения криминальной направленности) применяются программы, которые автономно позволяют осуществлять незаконный перевод денежных средств со счетов ничего не подозревающих компаний и граждан;

– рассматриваемым деяниям свойственна нетипичность, или нестандартность, действий преступников[1].

В отличие от обычных преступлений при совершении преступлений с использованием возможностей IT-технологий зачастую довольно трудно установить признаки объективной стороны деяния, не говоря уже про выявление, обнаружение и задержание преступников.

Исследователи выделяют отдельные трудности расследования преступлений, совершаемых с использованием возможностей IT-технологий:

– зачастую правоохранительным органам не сразу удается выявить сам факт правонарушения. Преступники с особой легкостью могут получить информацию, которая скрыта и об этом никто не узнает;

– степень причиненного вреда может быть очень значительна: злоумышленник может взломать базу данных какого-нибудь банка и снять денежные средства со счетов клиентов;

– преступник, который совершил деяние на территории России, может быть из любой точки мира;

– интеллектуальная составляющая данного вида преступной деятельности довольно высока. Как правило, преступники наделены незаурядным интеллектом, умеют хорошо скрывать следы, что создает сложности в борьбе против них.

Тактика производства допроса свидетелей при расследовании киберпреступлений напрямую зависит от многих факторов как позитивных, так и негативных. Опросы следователей, расследующих данную категорию дел, показывают, что они часто сталкиваются со сложностями при допросе. Около 71 % опрошенных указали, что чаще всего трудности возникают с терминологией,

[1] *Свистун С.Н.* Особенности проведения допроса (очной ставки) при расследовании киберпреступлений // Экономика и социум. 2017. № 8 (39). С. 26.

а также с выбором тактики воздействия и установлением контакта с допрашиваемым[1].

При подготовке к допросу и в ходе его проведения следователю необходимо обратить внимание, во-первых, на возможность привлечения специалистов, которые обладают специальными знаниями в сфере телекоммуникационных систем, компьютерных технологий и компьютерной техники, т. к. зачастую следователи не обладают такими знаниями или обладают ими в недостаточном объеме. Отсутствие специальных знаний у следователя обусловливает «интеллектуальное» противодействие расследованию со стороны преступника[2]. Во-вторых, на постоянную изменчивость сетевого пространства, которое в свою очередь определяется краткосрочностью существования и высокой изменчивостью отдельных видов доказательств, находящихся в электронной форме. При производстве допроса следователю целесообразно применять знания юридической психологии, поскольку именно применение психологических приемов позволяет расположить к себе допрашиваемого свидетеля и получить от него максимум информации. Также, готовясь к допросу свидетеля по киберпреступлениям, следователю необходимо обратить особое внимание на информационное обеспечение допроса и его планирование. Одной из наиболее важных составляющих является информационное обеспечение: чем оно технологичнее, тем выше степень контроля ситуации на допросе. Это в свою очередь позволит избежать ошибок в квалификации преступного деяния.

Положительно на выбор тактических приемов производства допроса влияет достаточная осведомленность следователя о типах и видах компьютерно-технических средств, использованных в качестве орудия совершения преступления.

Именно это обстоятельство, по общему правилу, обусловливает необходимость присутствия при производстве допроса специалиста в сфере компьютерных технологий, который уже на этапе подготовки к допросу может разъяснить следователю неясные технические термины, особенности устройства и принцип работы изъятых средств, возможные способы совершения преступлений посредством их применения.

---

[1] *Шевченко Е.С.* Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. 2016. № 10. С. 160–169.

[2] *Яковлев А. Н., Олиндер Н.В.* Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. М., 2012. С. 43.

Основной целью допроса при расследовании киберпреступлений является выявление (выяснение) информации, связанной с виртуальными следами, а также иной информации, имеющей отношение к расследуемому виду киберпреступления.

Как отмечалось выше, допрос свидетелей имеет тактические особенности, которые зависят не только от механизма совершения киберпреступлений, но и от криминалистического типа свидетелей.

Тактика производства допроса по уголовным делам этой категории напрямую зависит от специфики механизма совершения преступления и иных как позитивных, так и негативных факторов. К числу первых следует отнести наличие определенного объема информации о преступном событии, полученного из различных источников (в ходе предварительной проверки материалов о расследуемом событии, результаты оперативно-розыскных мероприятий), а также о лице, с которым предстоит производство следственного действия (полученной ранее в ходе его объяснений, из протоколов процессуальных действий). В число негативных факторов можно включить значительный промежуток времени, прошедший с момента совершения преступления до момента производства допроса[1].

Представляется обоснованной точка зрения В.М. Быкова, который считает, что тактика допроса должна строиться с учетом соответствующего криминалистического типа допрашиваемых. Им были выделены следующие типы: активные и неактивные, добросовестные потерпевшие, неустойчивые, недобросовестные потерпевшие[2].

Данную типизацию можно применить и к свидетелям. Так, например, допрашивая свидетелей, необходимо выяснить следующую информацию: какие компьютерно-технические средства использовались потерпевшим или подозреваемым; какими знаниями о компьютерно-технических средствах, их характеристиках обладают допрашиваемые; какими навыками работы на компьютере или технически сложном устройстве владеют. В процессе их допроса необходимо установить: местонахождение юридического лица, организационно-правовую форму и характер деятельности; режим деятельности юридического лица; содержание и объем информации, хранящейся в компьютере; кто из сотрудников и каким обра-

---

[1] *Смирнова И. Г., Коломинов В.В.* Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Известия Иркутской государственной экономической академии. Электронный научный журнал. 2015. Т. 6. № 3. URL: http//eizvestia.isea.ru.

[2] *Быков В.М.* Допрос потерпевшего / В.М. Быков // Законность. 2014. № 6. С. 27–32.

зом вступал в контакт с предполагаемыми преступниками и другое. Данный перечень зависит от конкретной типичной исходной следственной ситуации и не является исчерпывающим.

Таким образом, тактически значимая информация о личности киберпреступников при производстве допроса свидетелей должна быть направлена на установление и получение сведений об уровне технической подготовленности и компьютерных навыках подозреваемых; о возможных мотивах совершения киберпреступления; о дифференциации в зависимости от локализации преступной деятельности; об информации, размещенной в социальных сетях; о психологическом состоянии или информационных болезнях (зависимостях, фобиях) подозреваемых.

Тактика производства допроса по уголовным делам этой категории напрямую зависит от специфики механизма совершения киберпреступлений[1].

Таким образом, специфика расследования преступлений, совершенных с использованием возможностей IT-технологий, требует разработки новых тактических подходов и приемов к осуществлению такого следственного действия, как допрос, что, несомненно, позволит повысить эффективность расследования.

---

[1] *Маслакова Е.А.* Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Политика и право. 2014. № 1. С. 36.

Некоторые способы совершения преступной деятельности мошеннического характера с использованием платежных карт

М. Е. Репин
(УМВД России по г. Н. Новгороду)

В статье рассматриваются некоторые способы совершения мошенничества с использованием платежных карт; представлены современные технологии, которые используют мошенники для получения конфиденциальной информации о реквизитах подлинных карт и их держателях; делается определенный вывод о том, что знание основных методов и способов совершения преступлений данного вида обеспечит в будущем развитие эффективных механизмов и средств активного противодействия злоумышленникам, а также позволит повысить уровень знаний и грамотности населения об информационной безопасности.

Мошенничество, интернет-мошенничество, способ преступления, платежная карта, мошенничество с использованием платежных карт.

В современных условиях развития глобального общества и цифровой экономики одной из приоритетных задач, стоящих перед правоохранительными органами нашей страны, является борьба с преступной деятельностью в сфере компьютерной информации. Наступившее столетие демонстрирует стремительное развитие высоких технологий. Это стало отчетливо ясно уже на пороге XXI века. Одной из основных движущих сил развития общества и экономики стала информация, в том числе и компьютерная. Но в рамках информатизации, одновременно с прогрессом, наблюдается и рост преступности в сфере компьютерной информации. Так, по статистическим данным ГИАЦ МВД России, количество зарегистрированных преступлений в сфере компьютерной информации в 2012 г. составило 241, в 2013 г. – 258, в 2014 г. – 268, в 2015 г. – 280, в 2016 г. – 321[1].

Нарастающее развитие компьютерных технологий предполагает, с одной стороны, улучшение качества жизни общества, с дру-

[1] Главный информационно-аналитический центр МВД России [Электронный ресурс]: состояние преступности – статистика и аналитика. URL: https://xn—b1aew.xn—p1ai/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen (дата обращения: 01.04.2018).

гой – совершенствование механизмов подготовки, совершения и сокрытия компьютерных преступлений[1].

Преступники становятся все более технологически оснащенными и информационно осведомленными и подготовленными. Это, в свою очередь, прямо способствует развитию преступности в данной сфере, в том числе и транснациональной.

Данные опроса показывают, что по количеству жертв от компьютерных преступлений Россия занимает одну из лидирующих позиций[2].

В свете перехода нашего общества в сферу цифровой экономики среди преступлений, совершаемых в глобальной единой информационно-телекоммуникационной сети Интернет, особое внимание приковывает интернет-мошенничество, совершаемое с помощью платежных карт. Указанный вид преступной деятельности получил широкое распространение в мире криминала. Выявление и раскрытие преступной деятельности данного вида осложняется тем, что, как правило, о факте совершения мошеннических действий становится известно только спустя некоторое, зачастую продолжительное, время как субъектам расследования, так и самим жертвам. Все это объясняет высокую латентность преступлений этой категории. Во всем мире данная проблема является актуальной, требующей скорейшего и незамедлительного вмешательства со стороны правоохранительных органов. Так, согласно исследованиям, ежегодный ущерб, наносимый Европейскому союзу действиями киберпреступников, исчисляется миллиардами евро[3].

В условиях глобальной информатизации общества, развития информационных технологий и сферы цифровой экономики создание систем предоставления банковских услуг, активный рост числа различных интернет-магазинов, развитие электронных платежных систем способствует тому, что все в большей степени населе-

---

[1] *Репин М.Е.* Личность «компьютерного преступника» в контексте криминалистической характеристики преступлений в сфере компьютерной информации // Криминалистические средства обеспечения деятельности по выявлению и расследованию преступлений экономической и коррупционной направленности: сборник статей / [под ред. А.Ф. Лубина]. Казань, изд-во «Бук», 2017. С. 194–196.

[2] *Афанасьев А. Ю., Репин М.Е.* Уголовно-процессуальные и криминалистические особенности расследования киберпреступлений // Криминалистическое обеспечение раскрытия и расследования преступлений: материалы X всероссийского научно-практического круглого стола (Ставрополь, 26 февраля 2016 г.). Т. 1. Ставрополь, 2016. С. 12–13.

[3] Европейских хакеров будут сажать на срок от двух до пяти лет [Электронный ресурс]. URL: http: //www.ferra.ru/ru/techlife/news/2012/04/02/ europa-Hack-criminal/#.VYJZF_ntmko (дата обращения: 17.03.2018).

ние доверяет безналичным расчетам, часто забывая о том, что даже в виртуальных сетях действуют мошенники[1].

На сегодняшний день Российская Федерация по росту платежей посредством электронных платежных средств (банковские карты и электронные кошельки) входит в одну из самых активно развивающихся мировых стран. В исследовании, проведенном Euromonitor International, наша страна, несмотря на относительно невысокий уровень количества мошеннических операций с использованием платежных карт, характеризуется взрывным ростом их числа. Так, в период с 2012 г. по 2016 г. это соотношение увеличилось на 296 %[2].

В криминалистическом смысле мошенничество с использованием платежных карт можно определить как систему действий по подготовке, совершению и сокрытию хищения чужого имущества, основным содержанием которой является использование поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты для осуществления обмана уполномоченного работника кредитной, торговой или иной организации[3].

Анализируя положения ст. 159.3 УК РФ «Мошенничество с использованием платежных карт», предусматривающей уголовную ответственность за соответствующий вид противоправных действий, можно выделить следующую классификацию способов совершения преступления.

В зависимости от того, какая разновидность платежной карты была использована мошенником для совершения преступления: а) расчетная карта; б) кредитная карта; в) иная платежная карта. Конечной целью злоумышленников не является получение реквизитов банковской карты. Масштабные кражи баз платежных данных направлены на перепродажу полученных реквизитов карт и последующий вывод средств. Например, в сентябре 2016 г. были взломаны ресурсы корпорации Samsung Digital Electronics и похищены платежные данные 3,2 млн банковских карт клиентов компании. Средняя стоимость реквизитов одной банковской карты варьи-

---

[1] *Атаманов Р.С.* Основы методики расследования мошенничества в сети Интернет: автореф. дис. ... канд. юрид. наук. М., 2012. С. 28.

[2] Рост рынка безналичных платежей стимулирует активность мошенников [Электронный ресурс]. URL: http://bankir.ru/novosti/s/rost-rynka-beznalichnykh-platezhei-stimuliruet-aktivnost-moshennikov-10037437 (дата обращения: 10.04.2018).

[3] *Антонов И. О., Шалимов А.Н.* Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Серия: гуманитарные науки. 2013. Т. 155. № 4. С. 196–203.

руется от 1,9 долл. США до 5,3 долл. США. Таким образом, в случае успешной продажи базы данных, полученной в результате взлома ресурсов корпорации Samsung Digital Electronics, преступный доход мошенников мог составить более 6 млн долларов США [1].

В зависимости от личности преступника: а) криминальный обман уполномоченного работника торговой организации; б) криминальный обман уполномоченного работника кредитной организации; в) криминальный обман уполномоченного работника иной организации.

Также выделяется криминальный обман, совершенный в одиночку либо в составе организованной группы. В ст. 159.3 УК РФ указано два способа совершения такого мошенничества: с использованием поддельной или принадлежащей другому лицу платежной карты.

Мы, в свою очередь, придерживаемся точки зрения некоторых ученых-экономистов и экономистов-практиков, рассматривающих отдельные проблемы обеспечения безопасности в платежной сфере, которые предлагают следующую обобщенную классификацию некоторых способов мошеннических действий, совершаемых с банковскими картами:

а) использование карт, которые не были выданы держателю карты;

б) использование поддельных карт;

в) проведение транзакций с использованием реквизитов карт;

г) использование украденных или утерянных карт;

д) несанкционированное использование персональных данных держателя карты и информации по счету клиента;

е) другие виды мошенничества[2].

Следует отметить, что технические устройства, которыми орудуют мошенники, активно развиваются и модернизируются[3]. Так, большой популярностью среди преступников пользуются устройства, позволяющие незаметно для владельца карты получить конфиденциальную информацию. К таким устройствам относятся так называемые скиммеры (от англ. skimming) – это приборы, которые монтируют на банкоматы для считывания и копирования конфи-

---

[1] Мошенничество по банковским картам в Интернете [Электронный ресурс]. URL: http://www.crime-research.ru/analytics/Present_Fraud29/ Card Not Present Fraud (дата обращения: 11.04.2018).

[2] Центр исследований платежных систем и расчетов. Мошенничество в платежной сфере: Бизнес-энциклопедия. М.: Интеллектуальная литература, 2016. С. 234.

[3] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

денциальной информации с карты – это накладные клавиатуры, видеокамеры. Следует отметить новейшую технологию скимминга, называемую шиммингом (от англ. shimming), суть которой заключается в использовании очень тонких плат (0.1 мм), внедряемых мошенниками в банкомат через щель приёмника платежных карт, при этом все введенные данные карты будут считаны[1].

Распространенным видом социальной инженерии являются так называемые фишинг и вишинг. Ярким примером которых является рассылка электронных писем с просьбой указать свои пароли, счета и т. п. Ссылка в сообщении приведет пользователя на ложный сайт, где и происходит кража персональных данных владельца карты. При этом, спустя некоторое время, сайт удаляется и отследить злоумышленников бывает практически невозможно. Принцип действия вишинга отличается тем, что для его реализации используется мобильная телефонная связь – в смс-сообщениях содержится просьба позвонить на определенный номер, ввести номер банковской карты, PIN-коды или другую личную конфиденциальную информацию.

В заключение необходимо отметить, что интернет-мошенничество не стоит на месте; с каждым днем изобретаются все более изощренные методы совершения преступлений данной категории преступлений. Исследование и анализ современных способов мошенничества с использованием платежных карт очень важно в наше время, ведь результаты их исследований могут обеспечить в будущем развитие механизмов и средств эффективного противодействия мошенникам, а также это позволит повысить уровень знаний населения об информационной безопасности в эпоху развития цифровых технологий.

---

[1] О новом способе мошенничества [Электронный ресурс]. URL: http://bankcarding.ru/shimming-pogovorim-o-novom-sposobemoshe nnichestva (дата обращения: 11.03.2018).

Аналитическое сопровождение следственной деятельности

О. В. Рожко,
начальник следственно-экспертного факультета,
кандидат юридических наук, доцент
(Академия МВД Республики Беларусь)

И. Г. Мухин,
врио начальника кафедры,
кандидат юридических наук
(Академия МВД Республики Беларусь)

В статье обобщается опыт ряда стран Западной Европы по организации деятельности службы криминальных аналитиков. Выдвигается идея о необходимости создания аналогичных подразделений в системе следственных органов.

Транснациональные корпорации, компании, предварительное следствие, цифровая криминалистика, криминальный анализ, тактический анализ, стратегический анализ.

В 2012 г. свет увидело довольно интересное исследование группы ученых под руководством Джеймса Глаттфельдера из Федерального технологического института в Цюрихе под кричащим заголовком «Миром правят несколько бизнесменов»[1]. По утверждению ученых, 40 % мирового капитала контролирует «ядро» из 147 корпораций. Однако не этот факт вызывает интерес, а то, каким способом он был установлен. Для анализа экономических связей между организациями исследователи применили математическую модель анализа данных. При проведении исследования ученые использовали Orbis 2007 – базу данных, которая содержит информацию о 37 млн компаний и инвесторов по всему миру. Из них ученые выбрали 43 060 компаний, принадлежащих транснациональным корпорациям, и выявили их общие активы. На основе этих данных была построена модель распределения экономического влияния транснациональных корпораций, в том числе через владение фондами и участие в прибыли. В результате

[1] Миром правят несколько бизнесменов [Электронный ресурс] / Режим доступа: URL: https://www.kp.by/daily/25855.3/2823134 (дата обращения: 11.03.2018).

системного анализа ученые выявили так называемую сеть глобального корпоративного контроля, состоящую из 1 318 корпораций с взаимными владельцами: каждая из этих компаний тесно связана еще, как минимум, с двумя другими компаниями, а среднее число связей между ними равно двадцати. Дальнейшее исследование выявило ядро этой сети – еще более тесно связанную между собой группу «суперорганизаций», в которую вошли 147 компаний, причем их активы тесно пересекаются друг с другом, что позволяет им контролировать 40 % глобального корпоративного богатства. Таким образом, ядро из менее 1 % компаний фактически представляет собой глобальную экономическую «суперструктуру», которая контролирует почти половину мировой экономики[1]. Данный пример является хорошим свидетельством того, насколько ценным может быть анализ больших массивов информации с целью выявления устойчивых взаимосвязей между объектами поиска в различных сферах социальной действительности.

Несомненно, что данное утверждение актуально и для правоприменительной деятельности, в первую очередь для предварительного расследования и раскрытия преступлений. По сути, предварительное следствие представляет собой построение информационной модели преступного деяния, основанной на добытых доказательствах. Информационная природа следствия обусловлена процессом выдвижения и проверки следственных версий, базисом которых являются сведения о лицах, событиях и взаимосвязях между ними. При этом, когда мы ведем речь о преступных деяниях, в которые вовлечены десятки, а то и сотни субъектов, работающих на преступный результат (киберпреступность, наркотраффик, многоэпизодные мошенничества, экономические преступления и т. п.), выявление устойчивых связей между фигурантами позволяет не только проверить обоснованность той или иной версии, но и получить доказательства устойчивости и управляемости определенной организованной преступной группы. Согласимся с высказыванием Е. П. Ищенко о том, что любая сложная, а значит организованная деятельность группы людей как в процессе подготовки и совершения преступления, так и в посткриминальный период, невозможна без коммуникации между ее субъектами. Поэтому она оставляет следы в различных информационных массивах правоохранительных и иных государственных органов, частных предприятий, пере-

[1] 40 процентов мирового богатства контролируют 147 транснациональных корпораций [Электронный ресурс] // Режим доступа: URL: http://gtmarket.ru/news/corporate/2011/10/24/3685 (дата обращения: 11.03.2018).

возчиков, операторов мобильной связи, банковских учреждений, охранных предприятий и т. п. Вся эта сохраняемая и накапливаемая информация дает уникальные возможности для увеличения фактической базы расследования[1]. Возможность использования данной информации в целях расследования и раскрытия преступлений переводит ее в категорию «криминалистически» значимой информации. Можно смело утверждать, что на смену традиционной (т. н. «полевой») криминалистике приходит новая «цифровая криминалистика» со своими закономерностями отображения следов преступной деятельности, методами их поиска, изъятия и использования в процессе доказывания. Одним из таких новых методов цифровой криминалистики стал криминальный анализ, который получил широкое распространение в правоохранительных системах западных стран. Безусловно, опыт коллег из Западной Европы и США может быть полезен и для отечественной криминалистической науки. В данной статье мы приведем сведения, полученные авторами в ходе стажировок по обучению криминальному анализу в Республике Польша (2011 г. и 2018 г.), а также в ходе обучающих семинаров, проведенных специалистами из ФРГ (2009 г.).

Отметим, что криминальный анализ возник в США еще в 60-е гг. XX в., когда организованная преступность стала там реальной угрозой обществу. В выводах специальной президентской комиссии утверждалось, что методы борьбы правоохранительных органов с организованными преступными группами неэффективны и нуждаются в обновлении. С тех пор было разработано много исследовательских программ для ФБР и ЦРУ. Одна из них (известная как Анакапская научная программа) положила начало методу криминального анализа. На сегодняшний день словосочетание «криминальный анализ» ассоциируется с международной организацией IALEIA (InternationalAssociationofLawEnforcementIntelligenceAnalysts), объединяющей аналитиков из различных правоохранительных структур большинства государств мира. Она вырабатывает единые стандарты проведения криминального анализа для всех своих членов, осуществляет обучение и повышение квалификации аналитиков. Понятие «криминальный анализ» в Германии в течение десятилетий тесно связано с работой органов криминальной полиции, так называемой криминальной уведомительной службой (KPMD). Эта служба была создана с целью оперативного анализа

[1] *Ищенко Е.П.* Информатизация следственной деятельности – адекватный ответ современной преступности / Е. П. Ищенко, П. П.Ищенко, «LexRussica (Русский закон)». М., 2008. № 6. С. 1445–1460.

преступной деятельности «преступников-гастролеров». Каждое новое происшествие, которое происходило в том или ином регионе, регистрировалось в криминальной уведомительной службе, здесь же оно перепроверялось и сравнивалось с установленными идентичными происшествиями, что помогало следователям определить возможную взаимосвязь различных преступлений. Что касается польской полиции, то фактически все, что связано с криминальным анализом (и в более широком смысле – с криминальной разведкой), берет свое начало с 2000 г., когда в страну прибыли эксперты из Нидерландов и Великобритании и обучили первых 24 криминальных аналитика. Отдельной проблемой было обеспечение польских криминальных аналитиков надлежащими условиями работы, в краткосрочном доступе к программному обеспечению AnalystNotebook, которое является основным инструментом, поддерживающим работу аналитиков. Благодаря финансовой поддержке Европейского союза рабочие подразделения были оснащены аналитическим программным обеспечением. В 2001 г. первый курс криминального анализа был проведен уже польскими лекторами, хотя и при участии иностранных преподавателей. В этом же году первые отделы криминальной разведки были созданы в отдельных гарнизонах полиции (первый был создан в Кракове). Срок обучения криминальному анализу составляет, как правило, четыре недели, при этом обучение сотрудников правоохранительных органов осуществляется на безвозмездной основе (на возмездной основе криминальному анализу обучают в течение трех недель сотрудников гражданских служб безопасности). Следует подчеркнуть, что к сотрудникам, обучающимся по курсу «Криминальный анализ», предъявляются следующие требования: 3 года службы в практических подразделениях криминальной полиции, сдача психологического теста на предмет выявления аналитических способностей, тест на уровень интеллектуального развития (с тестами успешно справляются 2–3 кандидата из 10). Прошедшие испытания кандидаты направляются на собеседование в Управление уголовных расследований. Из прошедших собеседование создаются группы по 12 человек. Криминальный анализ подразделяется на два основных направления: тактический анализ и стратегический анализ. Стратегический анализ используется для анализа преступности в определенных сферах, создания типового портрета лиц, совершающих ту или иную группу преступлений, анализ методики расследования уголовных дел. Тактический анализ применяется аналитиками в следующих случаях: анализ конкретного дела; сравнительный анализ дел; анализ преступных групп; анализ личного профиля; анализ запросов следователей.

Криминальный анализ наиболее эффективен в рамках расследования конкретного уголовного дела. Так, оперативный сотрудник либо следователь, давая задание аналитику, должен предоставить максимальный возможный массив информации и четко сформулировать вопросы. Криминальный аналитик при помощи специального программного обеспечения анализирует полученную информацию, проводит логический анализ взаимосвязи заданных объектов. Эффективность криминального анализа в значительной степени повышается при использовании различных баз данных и биллинговых систем. Результатом работы криминального аналитика является составление наглядных схем взаимосвязей, что значительно упрощает раскрытие и расследование дел. В то же время криминальный аналитик представляет не только схемы и диаграммы, но и аналитическую записку с необходимыми пояснениями.

Следует отметить, что аналитики не занимаются оперативной или следственной работой (они не добывают сведения, не проводят следственные и иные процессуальные действия), а осуществляют исключительно анализ имеющейся в распоряжении органа уголовного преследования информации. Данные для криминального анализа получают из всех доступных источников: открытых, негласных, полицейских, иных органов правосудия (компьютерные базы данных и досье документов; материалы, имеющиеся в уголовном деле; данные официальной статистики; материалы газет, журналов, радио и телевидения и др.). Работая с данными, аналитик должен всегда учитывать степень достоверности информации перед тем, как интерпретировать ее. Соответствующая оценка должна указывать надежность источника и достоверность собственно информации. В полицейских ведомствах стран Евросоюза принято оценивать достоверность информации в зависимости от источника ее происхождения и возможности проверки полученной информации. Такая система оценки данных получила название «4х4 система». Преимущество данной системы оценки информации состоит в том, что каждая информация имеет свой код и является ее неотъемлемой частью. Это означает, что независимо от того, куда в дальнейшем следует информация, где и кем она обрабатывается, важен номер кода, который указывает на то каким образом будет обрабатываться информация. Так, источникам информации присваиваются обозначения в виде букв латинского алфавита: A, B, C, D (в некоторых странах – X). В зависимости от возможности проверки информации ей присваиваются значения от 1 до 4. Классификация источника: **A** – нет сомнения в личности / достоверности / и способностях источника, или источник был всегда надежен;

B – источник был почти всегда надежен; **C** – источник был во многих случаях не надежен; **D (X)** – источник не проверен, показаний не имеется. Классификация информации: **1** – информация из собственных (полицейских) наблюдений или она исходит от официальных органов и не подлежит сомнению; **2** –Информация не из собственных (полицейских) наблюдений, ноисточник имел прямой контакт с информацией; **3** – информация из показаний, которые подтверждаются другими лицами; **4** – информация из показаний, которые не имеют подтверждения. Таким образом, для каждой информации есть своя оценка, состоящая из одной буквы и одной цифры. На основании анализа информации аналитик систематизирует и упорядочивает сведения об отношениях людей, организациях, участках местности, телефонных контактах и т. д. Визуализация информации выполняется посредством составления матриц и диаграмм связей. Такая работа может быть выполнена как вручную, так и с использованием специализированного программного обеспечения (например, AnalystToolbox (IALEIA), Anacapa (AnacapaSciences Inc, США), i2 (IBM, США), RICAS (ХОГА, Украина)). Следующим этапом работы аналитика является интерпретация данных. В ходе ее аналитик делает логические выводы относительно преступной деятельности, ролей причастных лиц, применяемых ими методов и т. п. В криминальном анализе наиболее полезна индуктивная логика, поскольку информация фрагментарна, ее источники разнообразны, а лица, принимающие решения, слишком часто забегают вперед, пытаясь предсказать будущие события или тенденции. Аналитик должен изучать, насколько это возможно, всю доступную информацию, а затем, отталкиваясь исключительно от фактов, выдвигать гипотезы и давать оценки. В частности, он должен рассматривать следующие аспекты преступной деятельности: кто к ней причастен; что делают эти лица; как они это делают; где все происходит; когда это происходило или будет происходить; почему они так поступают. Гипотеза, выдвинутая криминальным аналитиком, дает теоретическую посылку, которую необходимо проверить, чтобы убедиться в том, является ли она правильной. Такой подход ориентирует сбор информации по наиболее важным параметрам, экономит время и деньги, улучшает взаимопонимание и координацию между сотрудниками. Сообщение результатов анализа происходит как в устной, так и письменной форме. Например, аналитик может провести краткое совещание (либо инструктаж) или же представить письменный отчет. Но, например, в Республике Польша аналитик всегда сопровождает письменный отчет устными пояснениями.

Подводя итог вышеизложенному, полагаем, что использование методов криминального анализа оправдывает себя по многоэпизодным и сложным, а также резонансным уголовным делам. В связи с этим представляется возможным учесть зарубежный опыт при совершенствовании следственной деятельности в рамках организационной структуры следственных подразделений. Создание службы криминальных аналитиков может качественно повысить уровень расследования названной категории уголовных дел. Однако при этом следует, в первую очередь, решить проблему межведомственного обмена информацией как с правоохранительными органами, так и с отраслевыми ведомствами. Кроме того, немаловажным фактором успешной деятельности подобного подразделения является необходимость отграничения функции криминального анализа от функций анализа статистической информации о показателях и динамике развития преступности, чтобы не подменять работу криминального аналитика работой криминолога.

Применение цифровых средств фиксации информации при производстве следственных действий

А. В. Ростовцев,
профессор кафедры,
кандидат юридических наук, доцент
(Московский университет МВД России
им. В. Я. Кикотя)

В статье рассматриваются правовые, организационные и методические вопросы использования цифровой фотографии при фиксации хода и результатов следственных действий.

Цифровая фотография, следственные действия, фиксация следов, изменения фотоизображений, графические редакторы.

Использование современных научно-технических средств и методов способствует быстрому и объективному раскрытию и расследованию преступлений. Одним из таких средств является фотография, которая применяется при производстве различный следственных действий: осмотр, обыск, следственный эксперимент и др.

В настоящее время сотрудниками экспертно-криминалистических подразделений органов внутренних дел, принимающих участие в производстве следственных действий, активно используются средства и методы цифровой фотографии. Она практически заменила «традиционную» пленочную, поскольку это перспективное направление судебной фотографии позволяет существенно расширить возможности фиксации изображения. В равной степени это относится и к изготовлению иллюстрационных таблиц, отражающих ход и результаты следственных действий.

Цифровая фотографическая технология разработана сравнительно недавно благодаря научно-техническому прогрессу. Она располагает рядом существенных достоинств по сравнению «традиционной» пленочной фотографией[1]. К таким преимуществам относятся следующие:

– оперативный просмотр снятых кадров позволяет быстро понять ошибки и переснять неудавшийся кадр;

[1] *Ростовцев А. В.* Применение цифровой фотографии при осмотре места происшествия: учебно-практическое пособие. М., 2008. С. 19.

– изображения готовы для обработки и тиражирования на компьютере, их не надо сканировать;

– форматы цифровых фотографий без сжатия (RAW) имеют больший динамический диапазон, чем лучшие фотопленки;

– долгое хранение фотографий на электронных носителях (при своевременном копировании на свежие носители в соответствии со сроком службы носителя) не приводит к ухудшению их качества;

– большинство цифровых фотокамер компактнее пленочных аналогов.

Цифровая обработка изображений позволяет существенно расширить возможности как запечатлевающей, так и исследовательской фотографии. Цифровые технологии позволяют решать широкий круг задач: проводить измерения по фотоснимкам объектов на месте происшествия[1], выявлять различные слабовидимые изображения в документах[2], проводить портретные исследования[3].

При переходе на цифровые технологии получения фотографических изображений обозначился широкий спектр правовых, организационных и методических проблем, требующих своего разрешения. Все это требует комплексного изучения проблем практического и теоретического плана, связанных с особенностями использования цифровой фотографии при производстве следственных действий.

В соответствии с нормами уголовно-процессуального права при производстве следственных действий могут применяться технические средства.

«Правомерность, допустимость применения – вот тот основной критерий, с позиций которого оценивается всякое новое технико-криминалистическое средство... При этом допустимость обычно понимается как непротиворечие применения криминалистического средства «духу и букве» закона... а «буква» закона никогда не может охватить всего непрерывно развивающегося арсенала средств и методов борьбы с преступностью»[4].

Относительная простота редактирования цифровых изображений позволяет не только скорректировать допущенные при фото-

---

[1] *Газизов В. А., Емышев В. С.* Перспективы использования фотограмметрии в экспертной и следственной практике // Криминалистические средства и методы в раскрытии и расследовании преступлений: матер. 2-й всеросс. науч.-практ. конф.: в 2-х ч. М., 2004. Ч. II. С. 213.

[2] *Четверкин П. А.* Некоторые подходы экспертного исследования слабовидимых изображений в документах методами цифровой обработки оптических сигналов // Известия ТулГУ. Тула, 2006. Вып. 16. С. 263.

[3] *Зинин А. М.* Руководство по портретной экспертизе: учебное пособие М., 2006. С. 208.

[4] *Белкин Р. С.* Избранные труды. М., 2008. С. 368.

съемке ошибки, но и использовать обработку изображений в криминальных целях. Сомнения в достоверности фототаблиц с иллюстрациями, изготовленными с помощью компьютерных средств, обусловлены возможностью внесения изменений в фотоизображения с помощью современных графических редакторов ACDSee, AdobePhotoshop, XnView и др.

Для цифровой фотографии актуально мнение Н. С. Полевого, который отмечал, что получение фотоснимка как источника доказательства слагается из комплекса действий как технического, так и процессуального характера. Несоблюдение правил, обеспечивающих как техническое качество, так и процессуальное значение, ведет к искажению действительности и, следовательно, обесцениванию снимков как доказательств[1].

Применение цифровой фотографии должно соответствовать, наряду с требованиями технического характера, также и требованиям уголовно-процессуального закона. Законодатель придает особое значение таким свойствам доказательств, как относимость, допустимость, достоверность и достаточность (ст.ст. 75, 88 УПК РФ). Все фотоснимки, фигурирующие в фототаблице, должны иметь непосредственно отношение к производству следственного действия. При этом техническое оборудование должно гарантировать объективность полученных результатов. Об этом свидетельствуют соответствующие нормативные документы: ГОСТы, сертификаты соответствия, лицензии и т. д. Условия получения, обработки и хранения изображений должны быть отображены в протоколе следственного действия в соответствии с требованиями УПК.

На фотоснимках должно быть отображено достаточное количество признаков у наблюдаемых объектов, которые имеют непосредственное отношение к проводимому следственному действию. При этом качество воспроизведения указанных признаков должно позволять проводить их полное и всестороннее исследование. Для необходимости повышения доказательственного значения цифровых фотоснимков в процессе судопроизводства и предлагается использование цифрового фотографического формата RAW как одного из средств решения данной проблемы[2].

Наряду с уголовно-процессуальным кодексом требования к иллюстративным материалам протоколов следственных действий

---

[1] *Полевой Н. С.* О процессуальном значении фотографических снимков, используемых при расследовании преступлений // Труды Высшей школы МВД СССР. М., 1957. С. 109.

[2] *Трущенков И.В.* Использование цифровой фотографии в криминалистических экспертизах: автореф. дис. ... канд. юрид. наук. М., 2011. С. 18.

в расширенном виде дублируют и ведомственные нормативные акты, например приказы МВД России. Согласно ним при использовании методов цифровой фотографии должны указываться вид, модель, производитель использованного аппарата, а также вид, наименование, версия программного обеспечения, режим получения и печати изображений.

ЭКЦ МВД России дважды издавал рекомендации об использовании цифровой фотографии[1]. Такие рекомендации и требования по указанию условий применения фотографических методов исследования способствуют использованию полученных фотоизображений в системе доказательств. Действительно, согласно ч. 2 п. 5 ст. 74 УПК РФ, протоколы следственных и судебных действий являются доказательствами. Нарушение или несоблюдение правил применения методов цифровой фотографии порождают сомнение в доказанности обвинения. Поэтому они могут быть исключены из процесса доказывания.

Таким образом, совершенствование тактических особенностей использования методов цифровой фотографии при производстве следственных действий дает возможность расширить возможности правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению преступлений.

---

[1] Об использовании цифровой фотографии. Информационное письмо ГУ ЭКЦ МВД России от 24.04.2003 № 37/11-1676; Об использовании цифровой фотографии. Информационное письмо ГУ ЭКЦ МВД России от 15.03.2007 № 37/21-1128.

Вариант привлечения к ответственности администратора сайта, нарушившего авторское право

А. П. Рыжаков,
профессор кафедры,
кандидат юридических наук, профессор
(Тульский филиал Международного
юридического института)

В статье рассматриваются проблемы привлечения к ответственности администраторов сайтов, незаконно использующих чужие произведения, и предлагаются пути их разрешения.

Авторское право, администратор сайта, доказательство, использование произведения, компенсация, скриншот.

Развитие цифровой экономики и информационного общества привело к тому, что студенты преподавателю говорят: «Зачем нам приобретать Ваши произведения? Мы их бесплатно скачаем на доступном для любого пользователя сайте». Если раньше авторы могли быть уверенными, что за их труд они получат определенное вознаграждение, то в настоящее время бумажный носитель «умер», а электронный «без зазрения совести» расхищается.

Бороться с этим современным российским явлением авторам можно, как минимум, двумя путями: а) используя положения п. 1 ст. 1301 ГК РФ и б) обращаясь в органы Следственного комитета РФ с заявлением о преступлении, предусмотренном ст. 146 УК РФ.

Но оба эти способа не просты в применении. На пути их реализации законодатель установил препятствия для уважающего законы автора.

Согласно п. 1 ст. 1301 ГК РФ в случаях нарушения исключительного права на произведение автор вправе требовать от нарушителя вместо возмещения убытков выплаты компенсации в размере от 10 тыс. руб. до 5 млн руб., определяемой по усмотрению суда, исходя из характера нарушения.

Но для заявления иска нужно знать место жительства администратора сайта. Между тем регистратор сайта этих сведений не дает. И автор лишается возможности рассмотрения иска в суде. Судебная практика идет по пути не вполне законного получения искомых сведений и нотариального заверения скриншотов экрана, на которых

фиксируется незаконное использование произведений. Но все это приводит к дополнительным затратам автора (а не правонарушителя), которые зачастую заставляют последнего не связываться с процедурой восстановления своих авторских прав. И как следствие – нарушение авторских прав не пресекается, а растет в геометрической прогрессии.

Таким авторам возможно указать, что они вправе обратиться в территориальные органы Следственного комитета РФ с заявлением о совершении преступления, предусмотренного ст. 146 УК РФ. Но и здесь на пути законопослушного автора возникает препятствие – вероятность привлечения к ответственности за заведомо ложный донос (ст. 306 УК РФ). Уголовная ответственность за незаконное использование объектов авторского права или смежных прав возникает только в случае совершения противоправного деяния, по меньшей мере в крупном размере (ч. 1 ст. 146 УК РФ), когда стоимость прав на использование объектов авторского права и смежных прав (экземпляров произведений или фонограмм) превышают 100 тыс. руб.

Между тем автор может сомневаться в цене принадлежащего ему авторского права. Полагая, что его стоимость следователем может быть оценена менее 100 тыс. руб., он допускает возможность рассмотрения уже в отношении него самого вопроса о привлечении к ответственности за совершение преступления, предусмотренного ст. 306 УК РФ. И вновь автор из-за этого отказывается от действий, которые, если бы они реализовывались гражданами по значительному количеству подобных фактов, они могли бы значительно снизить остроту проблемы повсеместного нарушения авторских прав.

Кто-то скажет, что только автор может определить стоимость принадлежащего ему права (в нашем случае авторского права). И если он считает, что стоимость этого права не менее 100 тыс. руб., то, по меньшей мере, привлечь его к ответственности за заведомо ложный донос нет оснований, даже когда следователь не согласен с мнением правообладателя (автора). Автор статьи не может не согласиться с такой позицией. Но позволим себе вновь напомнить о п. 1 ст. 1301 ГК РФ. Компенсация за нарушение исключительного права на произведение, которую автор вправе требовать от нарушителя вместо возмещения убытков не может быть меньше 10 тыс. руб. и более 5 млн руб. Таким образом, когда администратором сайта незаконно использовано 10 произведений, безусловно, имеет место крупный размер, т.к. стоимость нарушенного права на использование объектов авторского права составляет не менее 100 000 (10 000 х 10 = 100 000) руб. Причем не обязательно, чтобы

это были произведения одного автора. Состав преступления, полагаем, имеет место и тогда, когда администратор сайта незаконно использовал, к примеру, по одному произведению десяти авторов.

Итак, в предложенной ситуации авторам стоит объединиться и обратиться в местные органы Следственного комитета Российской Федерации с совместным заявлением (заявлением одного автора о незаконном использовании объектов авторского права, принадлежащих нескольким авторам). Причем в этом случае им не обязательно знать место совершения преступления. Автор вправе обратить в ближайший следственный орган СК России. Туда же следует представить скриншоты экрана, на которых им было зафиксировано незаконное использование их произведений.

Принявший заявление о преступлении орган предварительного следствия не сможет принять по нему процессуальное решение, не установив данные о лице, являющемся администратором сайта. Получив информацию о таковом, включая и место его жительства, следователь, скорее всего, направит заявление по подследственности.

Даже если по той или иной причине в последующем в отношении администратора сайта будет вынесено постановление об отказе в возбуждении уголовного дела, у автора появится возможность по его ходатайству ознакомиться с материалами данного производства, выяснить сведения об администраторе сайта, позволяющие обратиться в суд с требованием к нему о компенсации за нарушение исключительного права на произведение. И доказательствами здесь уже выступят не представленные автором в суд скриншоты, а истребованные судом из уголовно-процессуального производства скриншоты, послужившие основанием для принятия по итогам рассмотрения заявления о преступлении соответствующего процессуального решения.

И последнее, на что стоит обратить внимание лиц, чьи авторские права были нарушены. Даже в случае отказа в возбуждении уголовного дела по Вашему заявлению о преступлении у автора произведении есть право на рассмотрение его иска в рамках гражданского процесса. И тем самым автор, чьи права были нарушены, вполне может рассчитывать на гораздо большую, чем в рамках уголовного процесса, компенсацию за незаконное использование его произведения.

Организационно-тактические особенности обеспечения расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Е. Ю. Самолаева,
доцент кафедры,
кандидат юридических наук
(Московский университет МВД России
им. В. Я. Кикотя)

В статье рассматриваются проблемы практики организации расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Информационно-телекоммуникационные технологии, компьютерные технологии, расследование преступлений.

Повышение качества расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в настоящее время приобрело особое значение. С использованием информационно-телекоммуникационных технологий распространяется запрещенная информация (о наркотических средствах, оружии, взрывчатых веществах и др.), нарушается авторское право, совершаются преступления корыстной направленности, осуществляются призывы к противоправным действиям и др.

УК РФ содержит 20 составов, в которых информационно-телекоммуникационные сети являются либо предметом преступления (ст. 274, ч. 3 ст. 274.1 УК РФ), либо способом совершения преступления (ч. 1 ст. 137, ч. 1 ст. 159.1, ч. 1 ст. 171.2, ч. 1 ст. 185.3, ч. 2 ст. 205.2, п. «б» ч. 2 ст. 228.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2 , ч. 2 ст. 280, ч. 2 ст. 280.1, ч. 1 ст. 282 УК РФ и др.).

Опасность совершения преступлений с использованием информационно-телекоммуникационных технологий (в том числе сети Интернет) заключается в упрощении достижения преступником своей цели за счет анонимности его действий, простоты, быстроты и массовости использования телекоммуникационных сетей.[1] Так,

[1] *Косарев М.Н.* Информационно-телекоммуникационные сети как признак преступления // Вестник Уральского юридического института МВД России. 2014. № 4. С. 55–56.

блокировка 16 апреля 2018 г. только одного мессенджера Telegram показала высокую заинтересованность общества в такого рода «продуктах»[1]. При этом данный сервис не самый популярный. Количество его пользователей составляет 10–13 млн в России (в мире – более 200 млн)[2]. Для сравнения: число пользователей социальной сети Facebook в России превышает 14,4 млн (в мире составляет более 2 млрд), Instagram – более 22 млн (в мире – более 700 млн)[3].

Очень популярны приложения, которые позволяют отправлять собеседникам зашифрованные текстовые сообщения и файлы, которые будут безвозвратно удалены со всех устройств по истечении определенного пользователями времени (например, Wickr, Snapchat, Burn Note и др.).

В современном преступном мире социальные сети широко используются для реализации наркотических средств, потенциально опасных психоактивных веществ, оружия, совершения действий террористического характера. С их помощью распространяется информация о запрещенных к обороту предметах и веществах в целях поиска потенциального покупателя, мест их хранения с момента приобретения до момента передачи, доставки и др.

Исследование состояния преступности в данной сфере позволило отметить рост преступлений, совершаемых в сфере компьютерной информации (в 2017 г. на 7,7 % больше зарегистрировано, чем в 2016 г.), а также увеличение числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Так, в 2017 г. с использованием компьютерных и телекоммуникационных технологий было совершено 90 587 преступлений, что составляет 4,4 % от числа всех зарегистрированных в этом году преступлений. При этом их раскрываемость составила всего 24,4 %. Число раскрытых преступлений в сфере компьютерной информации также снизилось почти на 20 %[4].

---

[1] *Рожков Р., Новый В.* Блокировка Telegram приобрела рекордный масштаб // Комменсант.ru (от 17.04.2018) [Электронный ресурс]. Режим доступа: URL: https:// www.kommersant.ru/doc/3606044 (дата обращения: 18.04.2018).

[2] Статистика аудитории Telegram на январь 2018 [Электронный ресурс]. Режим доступа: URL: // https://telegram-region.com/statistika-auditorii-telegram-na-yanvar-2018/ (дата обращения: 20.04.2018).

[3] *Сергеева Ю.* Социальные сети в 2018 году: глобальное исследование [Электронный ресурс]. Режим доступа: URL: https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/ (дата обращения: 20.04.2018).

[4] Состояние преступности в России за январь – декабрь 2017 года. МВД России ФКУ «ГИАЦ» [Электронный ресурс]. Режим доступа: URL: http:// www.mvd.ru (дата обращения: 11.04.2018).

В связи с этим вопросы организации и тактики расследования преступлений данной категории особенно актуальны. Они требуют изучения для выявления причин такого снижения. В частности, во многих случаях уголовные дела о преступлениях, совершенных с использованием компьютерных технологий, не возбуждаются в связи со сложностью их квалификации и доказывания, а также малочисленной практикой их расследования.

Решение о возбуждении уголовных дел по фактам совершения уголовно-наказуемых деяний с использованием компьютерных технологий в основном принимается на основании материалов оперативно-разыскной деятельности. Положительный результат в области раскрытия подобных преступлений связан с правильной организацией взаимодействия с другими подразделениями и службами правоохранительных органов. Наиболее перспективные для расследования и дальнейшего направления в суд материалы связаны с задержанием лиц, совершавших данные преступления, в ходе реализации оперативной разработки.

После задержания следователю необходимо выполнить алгоритм действий, включающий следственные и процессуальные действия: составление протокола задержания; производство выемки предметов, которые могут использоваться для хранения, уничтожения, блокирования, модификации или копирования компьютерной информации (флеш-накопители, мобильные телефоны, портативные компьютеры); осмотры с участием специалистов изъятых предметов; обыски; направления органу дознания отдельных поручений о производстве следственных, оперативно-разыскных действий, направленных на выявление связей подозреваемого, установлению источников приобретения им имущества; допрос свидетелей; получение образцов для сравнительного исследования; назначение судебных экспертиз (судебные компьютерные экспертизы, фоноскопические, почерковедческие и др. судебные криминалистические экспертизы) и т. д.

Расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, предполагает деятельность следователя по сбору доказательств (ст. 86 УПК РФ) в рамках предмета доказывания (ст. 73 УПК РФ). Однако несмотря на урегулирование УПК РФ данных вопросов, правоприменительная практика складывается не единообразно.

Так, сложности в ходе расследования могут возникнуть с установлением времени и места совершения преступления. Наиболее наглядно это можно продемонстрировать на примере файлового хранения данных на носителе информации.

По данным следственной практики, временные атрибуты файла часто подвергаются фальсификации (посредством перевода часов вперед или назад или их остановки с использованием специальных программ)[1]. Такого рода действия затрудняют оценку достоверности сведений, содержащихся в файле документа, и не позволяют его использовать в качестве доказательства.

Сложнее устанавливать место совершения преступления в связи с тем, что в данных преступлениях им может признаваться не только традиционный его вид (физический адрес), но и часть информационного пространства (домен, сайт), в котором фактически было совершено преступление активным пользователем. Например, это сайт, который зарегистрирован на сервере, имеющем физическое местоположение, и лицо, его пользователь, находившийся в момент совершения преступления по конкретному адресу[2].

Также сложности в доказывании представляет использование доказательств в электронной форме. Текущие требования, предъявляемые к электронным носителям информации, состоят в том, что они должны быть в оригинальном, а не скопированном виде (п. 5 ч. 2 ст. 82, ч. 9.1 ст. 182 УПК РФ). В то же время позиция высших органов власти по данному вопросу – запретить следственным органам изымать серверы и жесткие диски при проведении следственных мероприятий (правда, на предприятиях, чтобы не приостанавливалась их деятельность)[3].

Осмотр электронного носителя информации трудоемок. Количество файлов на носителе может быть большим. Поскольку неизвестно изначально, какой файл может быть значим для расследования, фиксация информации, находящейся на носителе, обычно занимает достаточно много времени[4].

---

[1] *Першин А.Н.* Временные следы при расследовании преступлений, совершаемых с использованием компьютерных технологий // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. М., 2016. № 1. С. 46–51.

[2] *Чернышов В. Н, Лоскутова Е.С.* Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5. С. 199–203.

[3] Путин запретил следователям изымать серверы и жесткие диски на предприятиях // Вести. ru (от 03.08.2017) [Электронный ресурс]. Режим доступа: URL: http://www.vesti.ru/doc.html?id=2917073&cid=7 (дата обращения: 05.02.2018).

[4] *Сидоров В. В., Новиков А.А.* Особенности фиксации представленной информации в электронном виде криминалистически значимой информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2016. № 2 (44). С. 48–51.

Использование специальных познаний в сфере компьютерных технологий также занимает неотъемлемую часть расследования. Успех расследования напрямую зависит от тесного взаимодействия со специалистами и своевременного назначения судебной компьютерной экспертизы.

Следователь должен знать объект исследования данной экспертизы, ее разновидности, вопросы, которые можно поставить перед экспертом. Так, в науке приводится следующая разновидность компьютерных экспертиз: судебная аппаратно-компьютерная, судебная компьютерно-программная, судебная информационно-компьютерная экспертиза, судебная компьютерно-сетевая экспертиза[1]. На практике назначается в основном компьютерно-техническая[2].

В некоторых случаях следователь может принять решение не назначать экспертизу, а получить показания от специалиста, в частности провести осмотр объекта с его участием. Показания специалиста также могут быть положены в основу обвинения. Следователю только необходимо правильно определить, в каком случае это целесообразнее сделать.

Данный вопрос рассматривается в юридической литературе неоднозначно. Основная проблема заключается в содержании экспертизы (как исследования с целью решения поставленных вопросов) и осмотра (позволяющего обнаружить и зафиксировать компьютерную информацию)[3]. Не вызывает сомнения только тот факт, что при проведении данных следственных действий участие специалиста (эксперта) необходимо.

Знание правил работы с компьютерной информацией, позволяющих не допустить возможность ее потери, является одним из важных условий успешного расследования преступлений, совершенных с использованием компьютерных технологий. Поэтому если есть вероятность, что в ходе осмотра может быть уничтожена или повреждена информация, необходимо обязательно привлекать специалистов или назначить судебно-компьютерную экспертизу.

---

[1] *Васюков В.Ф.* Некоторые аспекты назначения судебной компьютерной экспертизы при расследовании хищений в сфере информационных и коммуникационных технологий // Вестник Удмуртского университета. Серия Экономика и право. 2016. Т. 26. № 4. С. 109–113.

[2] Решение по делу 1-106/2016: Приговор Советского районного суда г. Тамбов (Тамбовская область) по обвинению Полякова С. Е. по ч. 2 ст. 273 УК РФ [Электронный ресурс]. Режим доступа: URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tambova-tambovskaya-oblast-s/act-525703616/.

[3] *Пропастин С.В.* Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) // Современное право. 2013. № 6. С. 129–132.

В первую очередь это касается изучения неочевидных средств компьютерной техники и компьютерной информации (например, замаскированная сетевая карта) или необходимости разрешения идентификационных вопросов.

Также при производстве следственных действий специалист может подсказать, в каких случаях компьютерную технику необходимо осмотреть незамедлительно на месте ее обнаружения, чтобы не допустить потерю данных, хранящихся на компьютере (в некоторых случаях это может произойти при отключении его от сети). Это относится и к портативным мобильным устройствам (смартфонам), изъятым у подозреваемых. При выходе из программ или по прошествии определенного времени с момента прочтения сообщения или просмотра фотографии хранящаяся на устройстве информация может быть уничтожена.

В заключение отметим, что, не ощущая со стороны правоохранительных органов жесткого противодействия, лица, использующие современные технологии для совершения преступлений, будут стараться еще более активизировать свою преступную деятельность. В наших силах снизить подобную активность путем грамотной организации раскрытия и расследования подобного рода деяний, что невозможно без соответствующего методического обеспечения организационно-тактического характера, а также эффективного взаимодействия с другими ведомствами и службами.

Киберпреступность как форма экономической преступности

О. В. Сафронкина,
адъюнкт
(Воронежский институт МВД России)

В статье проводится аналогия между киберпреступлениями и преступлениями в сфере компьютерной информации.

Цифровая экономика, телекоммуникационные технологии, киберпространство, киберпреступления, экономические преступления.

В современном мире телекоммуникационные технологии являются одной из наиболее быстроразвивающихся областей.

Современная экономика развивается на основе новейших цифровых технологий обработки больших массивов данных, разработки новейших систем управления, что, в свою очередь, как отмечает Д. В. Удалов, приводит к изменению принципов конкурентных отношений[1]. Таким образом, конкурентная борьба все чаще происходит за формирование и благоприятное функционирование новых рынков товаров и услуг в интернет-пространстве.

Данное обстоятельство не могло остаться вне поля зрения преступного сообщества, идущего в ногу со временем и меняющего характер своих преступных посягательств в зависимости от текущего состояния и специфики киберпространства.

Анализируя современную преступность, можно ошибочно сделать вывод о том, что наиболее интеллектуальный вид преступности – экономические преступления – мигрируют в сторону киберпреступности, но если в этом разобраться более детально, сопоставить между собой эти два вида преступности, то можно обосновать неожиданный вывод: киберпреступность уверенно перерождается и приобретает форму экономической преступности.

В качестве примера рассмотрим DDoS-атаки (от англ. Distributed Denial of Service – «отказ в обслуживании») – это сетевые атаки – на сайт, перегружающие и выводящие его из строя путем подачи большого количества ложных запросов, то есть создающие такие условия, при которых пользователи системы не могут

[1] *Удалов Д. В.* Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1 (30). С. 12–18.

удаленно получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднен.

Чаще всего DDoS-атаки – это мера своеобразного высокотехнологичного экономического давления, представляющая собой воздействие на нормальное функционирование сайта, приносящего доход. Убытки от временного прекращения реализации товаров и услуг, затраты на восстановление работоспособности сайта, принятие мер по предотвращению последующих атак наносят существенный ущерб жертве. DDoS-атаки, как правило, почти всегда осуществляются по заказу недобросовестного конкурента и служат инструментом недобросовестной конкуренции.

Основными целями DDoS-атак являются блокирование возможности получения прибыли от использования сайта в некотором бизнес-процессе и автоматическое предоставление такой возможности конкурентам, а также получение части прибыли владельцев сайта в качестве откупа.

Ответственность за данное правонарушение может быть предусмотрена ст. 274 Уголовного кодекса Российской Федерации (далее – УК РФ) «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», а также рядом статей Уголовного кодекса РФ, в зависимости от совершенного деяния в каждом конкретном случае.

Проводя аналогию с экономическими преступлениями, такими как «Воспрепятствование законной предпринимательской или иной деятельности» (ст. 169 УК РФ), «Ограничение конкуренции» (ст. 178 УК РФ), «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» (ст. 183 УК РФ), «Воспрепятствование осуществлению или незаконное ограничение прав владельцев ценных бумаг» (ст. 185.4 УК РФ), можно сделать вывод о том, что целью их совершения и совершения DDoS-атак является устранение с потребительского рынка конкурентов либо получение откупа в целях последующего прекращения незаконных действий.

Целью иных преступлений в сфере компьютерной информации, ответственность за совершение которых предусмотрена ст. 272 УК РФ (неправомерный доступ к компьютерной информации) и ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ), является хищение информации, обладающей определенной ценностью, с последующей ее реализацией.

Кроме того, как поясняет руководитель проекта Kaspersky DDoS Protection в России Алексей Киселев, все чаще DDoS-атаки (ст. 274 и ст. 274.1 УК РФ) лишь отвлекают внимание IT-служб, чтобы осуществить кибератаку в то время, когда все силы брошены на восстановление работоспособности сайта, для хищения важных данных[1].

Эти преступления хорошо соотносятся с преступлением, предусмотренным ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», которое является экономическим преступлением и имеет аналогичную цель.

Обобщая сказанное, заметим, что киберпреступность и экономические преступления достаточно давно имеют существенным образом совпадающие цели[2]. Когда-то, на ранней стадии, законодатель криминализировал для первых преимущественно технологическую составляющую, а вторые лишь постепенно со временем адаптировал к особенностям информационных технологий. Однако когда экономика получила новое качество развития и стала цифровой, необходимость рассмотрения киберпреступности под иным углом зрения, как формы экономической преступности, стала востребованной.

Рассмотрим некоторые особенности экономических преступлений в условиях цифровой экономики, развитие которой определено Президентом Российской Федерации В. В. Путиным в качестве одного из приоритетов работы на ближайшую перспективу[3].

На пленарном заседании Совета Федерации РФ 11 апреля 2018 г. принято постановление о создании Совета по развитию цифровой экономики, важнейшей задачей которого является мониторинг деятельности субъектов РФ в направлении развития цифровой экономики[4].

Существенными особенностями цифровой экономики, на наш взгляд, будут являться блокчейн и криптовалюты. Блокчейн –

---

[1] *Киселев А.* Эксперт рассказал, сколько могут длиться DDoS-атаки [Электронный ресурс] // РИА Новости. М., 2018. URL: https://ria.ru/incidents/20180420/1519093666.html (дата обращения: 13.04.2018).

[2] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

[3] *Замахина Т., Кузьмин В., Латухина К.* Расширить пространство свободы. Послание Федеральному Собранию прозвучало мощно и убедительно [Электронный ресурс] // Российская газета – Столичный выпуск. 2018. № 7509 (46). URL: https://rg.ru/2018/03/01/o-chem-rasskazal-vladimir-putin-v-poslanii-federalnomu-sobraniiu.html (дата обращения: 13.05.2018).

[4] *Мисливская Г.* При Совфеде создан Совет по развитию цифровой экономики [Электронный ресурс] // Российская газета. 2018. URL: https://rg.ru/2018/04/11/pri-sovfede-sozdan-sovet-po-razvitiiu-cifrovoj-ekonomiki.html (дата обращения: 13.05.2018).

записи, удостоверяющие проведенные юридически значимые операции, – это одновременно некоторый аналог распределенных баз данных и в «чистом виде» цифровая информация. Криптовалюты – денежные обязательства в цифровой форме – также в «чистом виде» является цифровой информацией.

Безусловно, стоит ожидать, что очередным объектом преступного интереса в обществе с цифровой экономикой станут как раз блокчейн и криптовалюты. При этом для достижения экономического результата злоумышленники будут использовать «хакерские» и иные методы воздействия на цифровую информацию, которая является основой этих технологий. Если не адаптировать законодательство к этим новым особенностям киберпреступности и экономических преступлений, то одни и те же, по сути, действия будут квалифицироваться то как экономические преступления, то как киберпреступления, что не является допустимым.

Таким образом, тезис о киберпреступности как форме экономической преступности в обществе с цифровой экономикой имеет большие перспективы – и как направление совместного научного исследования этих форм преступности, и как повод для разработки новых подходов к структуре и содержанию уголовного законодательства.

Перспективные пути развития криминалистики в современных условиях

А. В. Сибилькова,
старший преподаватель,
кандидат юридических наук
(Московский университет МВД России
им. В. Я. Кикотя)

В статье рассматриваются пути улучшения состояния отечественной криминалистики, заключающиеся в проведении комплексных междисциплинарных исследований, интеграции современных информационных технологии в процесс раскрытия и расследования преступлений путем разработки программного комплекса моделирования личности неустановленного преступника, развитии конкретных практических рекомендаций, изучении зарубежного опыта и возможностей его использования в РФ.

Диагностическое исследование, криминалистическая характеристика преступления, криминалистическое моделирование, личность преступника, раскрытие преступления.

Проблема недостаточно высокой раскрываемости преступлений (около половины от всех зарегистрированных) остается в Российской Федерации актуальной год от года. Одной из основных задач криминалистики, наряду с расследованием и предотвращением преступлений, является их раскрытие. Современное состояние отечественной криминалистики критически оценивается учеными[1] и практическими работниками правоохранительных органов, отмечающими, что она перестала достаточно эффективно решать обозначенные выше задачи.

Пути улучшения состояния отечественной криминалистики видятся в следующем:

– проведение комплексных междисциплинарных исследований, направленных на обогащение криминалистики новыми знаниями, в том числе о человеке, как субъекте и объекте преступления;

[1] См.: *Волынский А. Ф.* Криминалистика и судебная экспертиза: современные проблемы развития, их причины, варианты решения // Актуальные проблемы судебно-экспертной деятельности в уголовном, гражданском, арбитражном процессе и по делам об административных правонарушениях: материалы VI Междунар. научно-практ. конф. Уфа, 2017. С. 41–49.

– интеграция современных достижений науки и техники, включая информатику и информационные технологии, в процесс раскрытия и расследования преступлений;

– приоритет развития конкретных практических разработок над теоретическими исследованиями;

– изучение зарубежного опыта и возможностей его использования в нашей стране.

При расследовании преступлений на первоначальном этапе основной задачей является установление личности преступника, которое ученые-криминалисты определяют как деятельность с использованием криминалистических методов и средств по обнаружению, фиксации, изъятию и исследованию следов преступления – источников информации, в том числе о свойствах и признаках лица, совершившего преступление, и формирование с их помощью знания о таком лице, осуществление его поиска на основе собранной информации[1].

В данном контексте речь идет о криминалистических диагностических исследованиях, под которыми понимается процесс установления природы или состояния диагностируемого объекта в ходе сравнительного исследования его признаков с соответствующими классификационными признаками диагностирующего объекта[2]. Следует отметить, что если методики диагностического исследования некоторых материальных следов активно развиваются и усовершенствуются (исследование биологических следов, пальцев рук, ног)[3], то некоторые диагностические методики разработаны еще в 60-х гг. XX в. и не претерпели с тех пор изменений, хотя очевидно, что условия жизни современного поколения людей существенно отличаются и это не может не сказаться на формировании их свойств.

---

[1] См.: *Зинин А.М.* Установление личности по признакам внешности (некоторые проблемные вопросы) // Уголовный процесс и криминалистика на рубеже веков: сб. науч. трудов. М.: Академия управления МВД России, 2000. С. 181; *Образцов В.А.* Выявление и изобличение преступника. М.: Юрист, 1997. С. 35; *Малыхина Н.И.* Криминалистические методы и средства установления лица, совершившего преступление: дис. ... канд. юрид. наук. Саратов, 2007. С. 24.

[2] См.: *Дубровин С.В.* Криминалистическая диагностика. М., 1989.

[3] См.: *Давыдов В. О.* К вопросу об эффективности использования методов генотипоскопии в сфере экспертной деятельности (на примере Экспертно-криминалистического центра Управления МВД России по Тульской области) [Текст] // Известия Тульского государственного университета. Серия: Математика. Механика. Информатика. 2013; *Тимофеева А.В.* Новый подход к установлению роста человека по следам его ног // Судебная экспертиза. 2010. № 1. С. 71–80.

Например, И. Н. Горбулинская, Е. А. Чебышева отмечают, что почерк современных людей имеет значительные отличия от почерков лиц, формирование которых происходило в других условиях. И, следовательно, существует необходимость разработки новой актуальной для сегодняшнего дня методики дифференциации почерка на мужской и женский[1].

Изучение автором научной литературы показало, что подобная ситуация сложилась и с методиками исследования следов зубов[2]. Нет свежих разработок, хотя очевидно, что в современных условиях применяются совсем другие методы лечения и протезирования зубов, а также ухода за ними, нежели 50 лет назад, что должно учитываться и при криминалистическом исследовании их следов.

Исходя из вышеизложенного, можно сделать вывод о том, что криминалистика остро нуждается в разработке современных методик диагностического исследования следов человека, а также в усовершенствовании способов применения получаемой в результате таких исследований криминалистически значимой информации.

Организацию и методику выявления, раскрытия и расследования преступлений необходимо рассматривать и исследовать в их органическом единстве как комплексную, междисциплинарную категорию, опираясь на современные достижения науки и техники, информационные технологии. Актуальной тенденцией развития информационно-аналитического программного обеспечения, способствующего расследованию и раскрытию преступлений, обладающего функционалом конвертации исходной, документированной информации, которая имеет свойство накапливаться в различных формах представления, является создание программного комплекса.

Результатом работы такого комплекса будет являться модель личности неустановленного преступника, основывающаяся на ранжировании информации об его свойствах и признаках. Она представляет собой таблицу, содержащую наиболее полный перечень признаков и свойств лица, совершившего преступление, в которой поисковая значимость свойств возрастает в строках снизу вверх, что способствует правильной организации работы с ними. Разрабатыва-

---

[1] См.: *Горбулинская И. Н., Чебышева Е.А.* Установление пола исполнителя рукописного текста, формирование которого происходило в современных условиях // Раскрытие и расследование преступлений: наука, практика, опыт: сборник научных статей. Вып. 1. Тула: изд-во ТулГУ, 2016. С. 34–38.

[2] См.: *Кузьменко Д.И.* Изменения зубочелюстной системы под влиянием вредных производственных факторов при производстве соляной кислоты: автореф. дис. ... канд. мед. наук. Кемерово, 1968; *Овруцкий Г. Д., Япеев А. С.* Кислотный некроз зубов. М., 1974.

ется данный программный комплекс на основании классификации свойств по частоте встречаемости среди лиц, совершивших аналогичные преступления, и возможности маскировки тех или иных признаков человека.

Применять такой программный комплекс предполагается для раскрытия и расследований преступлений, в результате совершения которых остаются материальные следы (чтобы можно было провести их диагностические исследования) и по которым возможна ситуация их совершения в условиях неочевидности.

Представляется перспективной разработка программного комплекса криминалистического моделирования личности неустановленного преступника по таким преступлениям, как убийство, причинение тяжкого вреда здоровью, изнасилование, насильственные действия сексуального характера, кража, разбой, мошенничество, вымогательство, фальшивомонетничество, незаконный оборот оружия, боеприпасов, взрывчатых веществ и взрывных устройств, незаконный оборот наркотических средств, психотропных, сильнодействующих и ядовитых веществ.

Такое разделение обусловлено тем, что для каждой категории преступлений распространенность тех или иных свойств среди совершающих их людей различна, поскольку связана со спецификой самого преступления. Например, состав такого преступления, как изнасилование, подразумевает, что в 100 % случаев его исполнителем является мужчина, а если говорить о таком привилегированном составе, как убийство матерью новорожденного ребенка, то в 100 % случаев его исполнителем является женщина. Мало преступлений, которые совершают мужчины и женщины в равных долях. Преступления, связанные с насилием (причинение вреда здоровью, убийство, грабеж, хулиганство и т. д.), как правило, совершаются мужчинами. Доля женщин высока среди лиц, совершивших иные преступления (мошенничество; присвоение или растрата; незаконное изготовление, приобретение, хранение, перевозка, пересылка, сбыт наркотических средств или психотропных веществ и др.). Такая же склонность к диспропорции касается и других свойств, присущих преступникам.

Как правило, при раскрытии и расследовании различных видов преступлений выявляется наиболее характерный набор свойств лиц, их совершивших, – это является одним из элементов криминалистической характеристики преступления, лежащей в основе методики расследования отдельных видов преступлений. При этом традиционно придается большее значение тому набору свойств, который встречается наиболее часто, чтобы следователь, исходя из него, выявил подозреваемых среди лиц, попадающих в поле зрения в ходе

расследования. Для методики криминалистического моделирования наибольшую ценность приобретает наличие у преступника свойств, которые являются редкими как для лиц, совершивших аналогичные преступления, так и для людей вообще, поскольку лицо, обладающее редким свойством, можно выделить среди большого количества людей, которые могут попасть в поле зрения сотрудников правоохранительных органов.

Реализация вышеупомянутых исследований соответствует приоритету решения конкретных практических задач над теоретическими исследованиями.

Если говорить об изучении зарубежного опыта и возможностей его использования в нашей стране, обращает на себя внимание метод когнитивного интервьюирования, разработанный за рубежом и еще мало исследованный отечественными учеными-криминалистами, под которым понимается метод получения достоверной, исчерпывающей личностной (субъективной) информации от потерпевших и свидетелей преступления о признаках внешности, поведении преступника (преступников) и обстоятельствах содеянного им (ими) на основе реализации системы приемов, базирующихся на достижениях когнитивной психологии[1]. В отечественной криминалистике он пока очень мало освещен, но, по нашему мнению, имеет необходимый потенциал для исследований и развития.

Цель когнитивного интервью состоит в том, чтобы при помощи определенных приемов активизировать память допрашиваемого лица и помочь ему тем самым вспомнить важные для дела факты, обстоятельства, признаки. Таких приемов четыре: мысленное, а затем вербальное воссоздание контекста события; детализация; припоминание обстоятельств в различной последовательности; смена перспективы.

Подводя итог сказанному, отметим, что несмотря на довольно часто звучащую справедливую критику состояния отечественной криминалистики, имеется потенциал для его улучшения, реализация которого видится в проведении комплексных междисциплинарных исследований, интеграции современных достижений науки и техники, включая информатику и информационные технологии, в процесс раскрытия и расследования преступлений, развитии конкретных практических рекомендаций, изучении зарубежного опыта и возможностей его использования в Российской Федерации.

---

[1] См.: *Образцов В. А., Богомолова С. Н.* Криминалистическая психология: учебное пособие для вузов. М.: ЮНИТИ-ДАНА: Закон и право, 2002. С. 384.

Особенности квалификации при расследовании создания, использования или распространения вредоносных компьютерных программ и программных продуктов

О.Х. Смаилов,
кандидат юридических наук
(Алматинская Академия МВД Республики Казахстан им. М. Есбулатова)

Статья посвящена анализу состава уголовного правонарушения, предусмотренного ст. 210 УК Республики Казахстан, влиянию его элементов на квалификацию деяний при расследовании уголовных дел.

Квалификация преступлений, вредоносные компьютерные программы, уголовная ответственность, состав преступления.

Создание и массовое производство компьютеров и иных технологических продуктов стало естественным продолжением движения человечества к более совершенному доступу к информационным ресурсам[1]. На сегодня данная информационная индустрия – это один из наиболее динамично растущих секторов мировой и национальной экономики. По состоянию на 2016 г. в Казахстане количество пользователей Internet составило более 12 млн человек (около 73 % населения страны).

Столь быстрое, но в то же самое время интенсивное развитие информационных процессов не могло не вызвать роста противоправных действий и проявления преступного интереса к выгодам современных технологий. Так, по данным американского Института компьютерной безопасности, в США продолжается рост компьютерной преступности: в 2014 г. году она выросла на 16 % по сравнению с 2013 г. При этом общая сумма причиненного ущерба составила 336 млн долл. США – на 36 % больше, чем в 2013 г.[2]

По результатам анализа обзоров Экспертной группы ООН по всестороннему комплексному исследованию проблем киберпреступности и ответных мер, принимаемых в странах-участни-

[1] *Громов Г.Р.* Очерки информационной технологии. М.: Яуза, 2013. 211 с.

[2] Рост компьютерной преступности в США // Компьютерная неделя (Computer Weekly). М., 2014. № 11.

цах и международном сообществе[1], можно отметить, что во многих государствах рост популярности Интернета пришелся на момент экономических, политических и демографических преобразований, сопровождающихся увеличением неравенства материального и социального положения, сокращением затрат в частном секторе и снижением финансовой ликвидности.

Криминалитет в своей преступной деятельности стал чаще использовать новые возможности совершения преступлений для получения личной или финансовой выгоды. В мире совершаются различные киберпреступления: действия, направленные на получение финансовой выгоды; действия, связанные с компьютерным контентом; действия, предпринимаемые с целью нарушения конфиденциальности, сохранности или доступности компьютерных систем; кибертерроризм и пр. Свыше 80 % преступлений с применением информационно-коммуникативных технологий являются результатом организованной преступной деятельности в киберпространстве, в основе которой лежит определенная последовательность операций по созданию вредоносных программ, заражению компьютеров, управлению бот-сетями, сбору личной и финансовой информации, продаже данных и «обналичиванию» финансовой информации и пр.

Противоправные действия, связанные с использованием компьютерных либо телекоммуникационных технологий, являются специализированной частью преступной деятельности в сфере информатизации и связи, направленной на нарушение прав и гарантий личности, общества и государства.

Так, зарубежный и отечественный опыт правоохранительных органов[2] убедительно свидетельствует, что противоправные действия с компьютерной информацией могут быть элементом действий:

– по несанкционированному прослушиванию радиомодемных, волновых, проводных, цифровых, аналоговых и с иных каналов связи, переговоров по абонентским устройствам связи, сообщений, передаваемых различными способами на расстоянии с использованием современных технологий;

– по неправомерному контролю почтовых сообщений и отправлений, незаконному изготовлению, производству, сбыту или приобретению специальных технических средств, предназначенных для

[1] *Чекунов И.Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дис. ... канд. юрид. наук: 12.00.08. М.: Московский университет МВД России, 2013. 223 с.

[2] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

негласного получения информации, по изготовлению в целях сбыта или сбыт поддельных кредитных и иных платежных и расчетных документов в тех случаях, когда они позволяют получить неправомерный доступ к информационному оборудованию;

– по нарушению неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, изобретательских и патентных прав в части разглашения без согласия автора или заявителя сущности изобретения, по разглашению тайны усыновления (удочерения) и др.;

– по незаконному получению, разглашению или использованию сведений, составляющих коммерческую либо банковскую тайну, тайну предоставления микрокредита, тайну коллекторской деятельности, а также информации, связанной с легализацией имущества.

Данные преступные деяния могут быть частью действий:

– по отказу в предоставлении гражданину информации;

– по сокрытию информации об обстоятельствах, создающих опасность для жизни или здоровья людей;

– по противоправному экспорту технологий, научно-технической информации и услуг, используемых при создании оружия массового поражения, вооружения и военной техники;

– по принуждению к совершению сделки или к отказу от ее совершения.

Введение отдельной главы «Уголовные правонарушения в сфере информатизации и связи» в Особенную часть Уголовного кодекса Республики Казахстан принятого 3 июля 2014 г., является той необходимостью, которую требует наша современность. Общественная опасность рассматриваемых в данной главе уголовных правонарушений заключается, прежде всего, в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи.

Киберпреступникам больше не требуется обладание сложными навыками или технологиями. Например, в развивающихся странах появились субкультуры молодых людей, занимающихся финансовым мошенничеством с применением компьютерных технологий. Многие из них еще подростками были вовлечены в совершение киберпреступлений.

Однако государственные органы и предприятия частного сектора воспринимают соответствующие риски и угрозы неоднозначно.

В настоящее время статистика преступлений, занесенных в полицейскую картотеку, не может служить основой для сравнения ситуации в разных странах, хотя такие статистические данные часто имеют большое значение при разработке национальной политики. Системы ведения статистики полицейскими органами в двух третях стран считаются неудовлетворительными для регистрации преступлений. Данные о преступлениях, зарегистрированных правоохранительными органами, зависят от уровня развития государства и профессионализма представителей правоохранительных структур и не всегда отражают реальные факты.

В недавнем прошлом Ирландская республиканская армия в Великобритании создавала специальные группы хакеров, в задачи которых входили взлом банковских счетов и похищение денег для финансирования этой террористической организации, а также сбор информации в Сети для будущих терактов. Многие хакерские группы, такие как югославская «Черная рука», пакистанская «G-Force» или палестинская «Unix Security Guard», не сделав ни единого выстрела, своими кибератаками наносили столь серьезный ущерб институтам государственной власти ряда стран, что заняли «достойное» место в списках террористических организаций. Не меньше проблем для законопослушных граждан создают и киберпреступления общеуголовного характера, совершаемые, например, с причинением материального или морального вреда, добывания тех или иных сведений ограниченного доступа (в том числе составляющих тайну частной жизни) из познавательных, а зачастую и из хулиганских побуждений[1].

Данная ситуация наблюдается и в нашем государстве. Так, 12 мая 2017 г. компания NCOC, разрабатывающая в Атырауской области морское месторождение Кашаган, стала одной из многих компаний в мире, подвергшихся кибератаке с использованием вредоносной программы WannaCry. Данная атака не оказала влияния на производственные операции, связанные с добычей нефти. Также не возникло проблем с обеспечением производственной безопасности. В качестве превентивной меры был прекращен доступ к Интернету и корпоративной почте. Кибератака затронула 10–20 % сервера и компьютеров кампании NCOC[2].

---

[1] *Журавленко Н. И., Шведова Л. Е.* Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. 3 (53). С. 66–70.

[2] На Кашагане усиливают систему безопасности в связи с кибератакой // URL: http://www. zakon. Kz (дата обращения: 07.07.2017).

Отечественная практика борьбы с уголовными правонарушениями в сфере информатизации и связи, несмотря на непродолжительное время функционирования уголовного законодательства Республики Казахстан, хотя и в незначительных объемах, но уже имеется.

Несомненно, что важной проблемой является повышение уровня специальной криминалистической подготовки следственных работников, непосредственно осуществляющих процесс правоприменения уголовного закона в рамках осуществления досудебного расследования.

Действующим уголовным законом предусмотрена ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК), неправомерные уничтожение или модификация информации (ст. 206 УК), нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК) и др.

Согласно диспозиции ч. 1 ст. 210 Уголовного кодекса Республики Казахстан объективная сторона предусмотренного ею деяния включает в себя совершение следующих альтернативных действий с вредоносными компьютерными программами и программными продуктами:

– создание компьютерной программы или программного продукта;

– внесение изменений в существующую программу или программный продукт;

– использование таких программ или продуктов;

– распространение таких программ или продуктов[1].

Вредоносность компьютерной программы или программного продукта заключается в том, что они способны и специально предназначены несанкционированно уничтожать, блокировать, модифицировать, копировать информацию, имеющуюся на компьютере, либо нейтрализовать средства ее защиты.

В настоящее время самыми распространенными являются программы, предназначенные для сбора информации, и программы для несанкционированного доступа к компьютерам либо другим программам. «Компьютерные вирусы» – это программы, которые умеют воспроизводить себя в нескольких экземплярах,

[1] Уголовный кодекс Республики Казахстан: практическое пособие. Алматы: изд-во «Норма-К», 2017. 240 с.

модифицировать (изменять) программу, к которой они присоединились, и тем самым нарушать ее нормальное функционирование, создаваемые злоумышленниками в целях получения какой-либо выгоды, принцип действия которых может быть разнообразным: от несанкционированного получения доступа к информации и дальнейшего его незаконного использования до побуждения пользователей совершать какие-либо действия в свою пользу. Известны следующие виды компьютерных вирусов: «червь», программы-шпионы, троянские программы, программа-блокировщик (баннер), загрузочные вирусы, эксплойт, фарминг, фишинг, руткит и многие др.

С объективной стороны уголовное правонарушение, предусмотренное ст. 210 УК РК, представляет собой «факт создания вредоносной компьютерной программы либо внесение изменений в существующие компьютерные программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию, использованию информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушению работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта»[1].

Состав уголовного правонарушения, предусмотренного ч. 1 ст. 210 УК РК, по конструкции объективной стороны является формальным, т. е. не требующим наступления последствий. Уголовная ответственность возникает уже в результате создания вредоносных компьютерных программ либо программных продуктов, независимо от того, использовались они или нет. По содержанию диспозиции ст. 210 УК РК само наличие исходных текстов вредоносных компьютерных программ и программных продуктов является основанием для привлечения к уголовной ответственности. Однако при этом следует учитывать, что в ряде случаев использование подобных программ не является уголовно наказуемым. Данное положение относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих лицензию на деятельность по защите информации. Формой деяния совершения уголовного правонарушения по ст. 210 УК РК может быть только

[1] *Бимолданов Е. М., Цой А. Н., Цой О. Р. и др.* Уголовные правонарушения в сфере информатизации и связи: учебное пособие. Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан, 2015. 194 с.

действие, выраженное в виде создания вредоносных компьютерных программ и программных продуктов, внесения изменений в уже существующие компьютерные программы, а равно умышленные использование и (или) распространение такой программы и программного продукта. Распространение электронных носителей с такими компьютерными программами или программного продукта предполагает перемещение их по сетям с предоставлением доступа к ним неограниченному кругу лиц, а также передачу носителей такой программы или продукта.

Субъективная сторона уголовного правонарушения, предусмотренная ч. 1 ст. 210 УК Республики Казахстан, характеризуется виной в виде прямого умысла. Уголовная ответственность, как определено в этой статье, наступает, если создание вредоносных программ или продукта либо внесение в них изменений заведомо для создателя программы преследовало цели неправомерного уничтожения, блокирования модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций[1].

В ч. 2 ст. 210 УК РК предусмотрены квалифицирующие признаки за совершение уголовного правонарушения:

1) группой лиц по предварительному сговору;

2) с использованием своего служебного положения;

3) в отношении государственных электронных информационных ресурсов или информационных систем государственных органов.

По части 3 рассматриваемой статьи в качестве особо квалифицирующих признаков предусмотрено:

1) совершение преступной группой;

2) повлекшие тяжкие последствия.

Субъект уголовного правонарушения – общий, физическое вменяемое лицо, достигшее 16-летнего возраста. Специальный субъект предусмотрен по п. 2 ч. 2 ст. 210 УК РК.

В заключение следует отметить, что если создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации,

[1] *Борчашвили И.Ш.* Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (т. 2). Алматы: Жеты жаргы, 2015. 1120 с.

копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта было условием совершения лицом другого уголовного правонарушения, деяния должны быть квалифицированы по совокупности вне зависимости от степени тяжести другого преступления.

Способы фальсификации отпечатков пальцев рук, используемые для неправомерного входа в смартфоны

Н. Э. Соловьева,
студентка
(юридический факультет ННГУ им. Лобачевского)

К. А. Пещерова,
студентка
(юридический факультет ННГУ им. Лобачевского)

В статье рассматриваются проблемы надежности биометрических систем, используемых для защиты информации на телефонных устройствах, на основе изучения возможных неправомерных способах входа в смартфоны.

Искусственные папиллярные узоры, спуфинг, биометрические данные, дистанционная идентификация, идентификация.

В современном быстроразвивающемся мире информационных технологий и компьютерных технических средств[1] закономерен интерес – как в научном, так и практическом аспекте – к проблеме создания искусственных папиллярных узоров (ИПУ). Фальсификация отпечатков папиллярных узоров пальцев рук ставит перед криминалистами и самим следователем ряд диагностических задач, связанных с выявлением возможных способов применения этих искусственных моделей. Но прежде чем разработать различные методики, рекомендации по выявлению данных фальсификаций и способах защиты данных в смартфонах, необходимо разобраться в способах создания этих искусственных папиллярных узоров и использования их для неправомерного вхождения в смартфоны других лиц.

[1] *Яковлева А. В., Алабердеев Р. Р., Андросов С. М., Афицинский В. А., Бабак Ю. Н., Баширова Н. В., Беспалько А. А., Бойко М. В., Бурбело О. А., Быкова К. В., Гапоненко А. В., Гассий В. В., Герасимов А. В., Головко М. В., Долинко В. И., Еськов С. В., Злобина И. В., Калинина Н. Н., Камкия Б. А., Кизим А. А. и др.* Механизм экономико-правового обеспечения национальной безопасности: опыт, проблемы, перспективы. Краснодар, 2012.

В настоящее время перспективным направлением считается биометрия (biometric), которая предусматривает удобные, надежные и дешевые средства идентификации (или подтверждения личности) и может использоваться без дополнительного контролирующего участия человека, в том числе при дистанционной идентификации.

Наибольшее распространение в биометрических системах контроля и управления доступом получил дактилоскопический метод (анализ отпечатков пальцев), который уже длительное время успешно использовался в криминалистике[1]. Выбор именно этой разновидности биометрии обосновывается требованиями по достаточной надежности, экономичности и скорости идентификации. Дактилоскопический метод, обосновывая свою актуальность, включает в себя постулаты о том, что не существует людей с одинаковыми отпечатками пальцев (даже у близнецов они различны), папиллярный узор, сформировавшись на эмбриональном уровне, не меняется на протяжении всей жизни и способен к саморегененрации при различных повреждениях. По данным International Biometric Group, доля систем распознавания по отпечаткам пальцев составляет примерно 52 % от всех используемых в мире биометрических систем[2]. По заявлению производителей и разработчиков данных биометрических систем, главным достоинством представляется в невозможности создания идентичного отпечатка папиллярного узора; высокой скоростью считывания и обработки данных; вероятность ошибочной идентификации составляет 0,000000001 %.

Биометрический процесс использования включает в себя следующую технологию: отпечаток, полученный с помощью специального сканера, датчика или сенсора, преобразуется в цифровой код и сравнивается с ранее введенным эталоном (особенности папиллярного узора преобразовываются в уникальный код, который сохраняет информативность изображения отпечатка). Методы опознания отпечатка пальца основаны на сравнении с образцами (рисунками потоков папиллярного узора) или на использовании характерных деталей папиллярных узоров. Некоторые системы

[1] *Ефременко Н.В.* Особенности современного криминалистического исследования пальцев рук / Н.В. Ефременко, А.С. Башилова // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов: тез. докл. Междунар. науч.-практ. конф., посвящ. Дню белорус. науки. Минск, 21 янв. 2011 г. / Акад. М-ва внутр. дел Респ. Беларусь; под ред. В.Б. Шабанова. Минск, 2011. С. 50–52.

[2] Подделка отпечатков пальцев [Электронный ресурс] // Новости hi-tech. 2017. Режим доступа: URL: http://www.techportal.ru/glossary/poddelka-otpechatkov-palcev.html (дата обращения: 16.03.2018).

успешно комбинируют оба метода. При опознании по образцу в базе хранятся отобранные части образа отпечатка пальца. Распознающий алгоритм выбирает те же самые области только что введенного отпечатка и сравнивает с имеющимися данными для установления подлинности.

При опознании по деталям папиллярных узоров из образа извлекаются только специфические места, где найдены детали папиллярного узора в виде начала (окончаний), разветвление (слияние) папиллярных линий, точки, мостик и т. д. Содержание шаблона в этом случае составляют относительные координаты и сведения об ориентации деталей папиллярного узора. Распознающий алгоритм отыскивает и сравнивает между собой соответствующие детали папиллярного узора. Ни поворот отпечатка пальца, ни его параллельный перенос (сдвиг) не влияют на функционирование системы, поскольку алгоритм работает с относительными величинами.

Рассмотрев процесс формирования биометрических систем и их достоинств, можно сказать, что мир информационных технологий не стоит на месте. Появились новые средства репрографии и копировальных материалов (перчатки, пластинки и др.), которые с высокой степенью точности могут воспроизвести папиллярные узоры пальцев рук определенного человека. Использование этих моделей могут способствует преодолению идентификационных биометрических систем защиты. Все это приводит к тому, что возникает вопрос о надежности данных биометрических систем, именно этим и пользуются преступники для получения доступа к личным данным граждан, к получению секретной информации[1].

В XXI в. поддельный отпечаток пальцев не является ценностью, существует даже специальный термин «SpooFing», обозначающий идентификацию по муляжу пальцев[2].

По мнению многих авторов, на данном этапе существуют основные способы, которые используются для изготовления искусственных отпечатков пальцев: использование пластических масс; метод фотолитографии; фотополимерный способ; лазерное гравирование на резине; флеш-технология; вулканизация резины с матриц, полученных на основе использования твердых фотополимерных композиций.

---

[1] *Моисеева Т. Ф.* Комплексное криминалистическое исследование потожировых следов человека: моногр. / Т. Ф. Моисеева. М.: ООО «Городец-издат», 2000. С. 13.

[2] Искусственные отпечатки пальцев для iPhone 5S [Электронный ресурс] // Новости в мире. 2015. Режим доступа: URL: https://xakep.ru/2014/01/26/fingerprint-iphone-5s (дата обращения: 28.03.2018).

На наш взгляд, одной из главных проблем, существующих на этом этапе, заключается в том, что использование отпечатков пальцев как способа защиты своих данных в телефоне является очень ненадежным, все это доказывают случаи простого изготовления копий как в зарубежных странах, так и в России. Например, в 2002 г. на конференции по безопасности Международного Союза телекоммуникаций в г. Сеуле аспирант Национального университета г. Йогамы в области криптографии Цутому Мацумоту описал две технологии изготовления искусственных папиллярных узоров на основе пластических масс и методов цифровой обработки информации, которые применялись им для обмана сенсоров отпечатков пальцев рук, используемых в системе безопасности. Именно эти две технологии и нашли свое применение для входа в системы по поддельным отпечаткам (разблокировка телефонов для получения информации, содержащейся в его базе данных).

В 2014 г. в Германии на конференции Chaos Communication Congress (конференция хакеров) в своем докладе Ян Крисслер (в мире известен как Starbug) показал работу своего метода по взламыванию сканеров отпечатков пальцев и использовал для этого только лишь фотографии хорошего качества с высоким показателем разрешения. Данный метод он продемонстрировал на примере фотоснимка большого пальца министра обороны Урсулы ван дер Ляйен, который был сделан на расстоянии трех метров от министра с помощью фотоаппарата, фокусное расстояние объектива составляло 200 мм, причем министр об этом не знал. Данные снимки позволили получить информацию об основных физических параметрах пальца министра обороны. Далее хакер с помощью программы для создания копий отпечатков пальца по фотографиям VeriFinger получил изображения, которые в последующем можно нанести на искусственно созданный палец.

Данные примеры еще раз доказывают незащищенность наших средств связи, если мы используем для них биометрические пароли. Еще один способ, которым пользуются преступники для неправомерного вхождения в телефоны, также был разработан Яном Крисслером осенью 2013 г. Когда на мировом рынке 20 сентября 2013 г. поступил в продажу IPhone 5S с сенсором TouchID, 21 сентября хакер Крисслер уже смог обойти систему и произвести копию отпечатка пальца пользователя гаджета. Этот отпечаток он взял с экрана поверхности Iphone. Процесс создания им дубликата был выложен в социальную сеть Youtube. Для производства поддельного отпечатка он использовал клей для дерева и графен, после чего полученную копию применял для создания «дубликата» пальца. При помощи

этого фальшивого пальца в дальнейшем можно было снять блокировку с iPhone. Посмотрев данное видео, никому не составит труда произвести поддельную копию.

Через две недели после этого хакерского приема также в Германии Берлинская организация *Security Research Labs* рассказала о методе, с помощью которого можно быстро обойти два защитных механизма iOS – удаленное стирание данных («remote wipe») и сенсор Touch ID в iPhone 5s[1]. Для решения этих задач необходима копия отпечатка пальца владельца очень хорошего качества с высоким разрешением. Только в данном случае отпечаток научились снимать прямо с экрана устройства. Данный способ подделки очень кропотливый и требует продолжительного доступа хакера к взламываемому устройству. Таким образом, самыми часто используемыми способами на сегодняшний день остаются следующие.

Первый получил название «контактный». Данный метод основывается на том, что образец отпечатка папилярных узоров пальца снимается с поверхности, на которой его оставил пользователь. При этом поверхность должна быть идеально гладкой, например это стекло смартфона.

Второй способ базируется на использовании цифровой фотографии. Данный метод имеет ряд особенностей. Во-первых, необходимо иметь техническое оснащение, которое позволяет создавать фотоизображения высокого качества. Во-вторых, владеть технической грамотностью для дальнейшей обработки фотоизображения. В-третьих, при фотографировании ладони необходимо выбирать такой ракурс, чтобы в дальнейшем полученное фотоизображение было пригодным для изготовления образца отпечтатка пальца[2].

Данные способы показывают простую технологию, позволяющую войти в телефонное устройство другого человека. И это приводит к тому, что хранение информации на защищенном устройстве функцией Touch ID не дает полной уверенности в том, что нашей информацией не завладеет какой-либо злоумышленник. На практическом примере проиллюстрируем, как можно самим воспроизвести отпечаток пальца и с помощью него войти в «запаролленное» телефонное устройство: для этого необходим пластичный материал (нами был использован кусок пластилина, но для достижения луч-

---

[1] Искусственные отпечатки пальцев для iPhone 5S [Электронный ресурс] // Новости в мире. 2015. Режим доступа: URL: https://xakep.ru/2014/01/26/fingerprint-iphone-5s (дата обращения: 28.03.2018).

[2] Подделка отпечатков пальцев [Электронный ресурс] // Новости hi-tech. 2017. Режим доступа: URL: http://www.techportal.ru/glossary/poddelka-otpechatkov-palcev.html (дата обращения: 16.03.2018).

шего результата рекомендуем использовать зубоврачебные слепочные массы), на который необходимо приложить палец и держать в течение 5 минут для полного отображения узора, имеющегося на пальце. Далее этот кусок необходимо заморозить и залить туда разведенную смесь пищевого желатина и отправить на несколько минут в морозильную камеру. В итоге получается объемный слепок отпечатка пальца, который позволил войти в систему телефона, защищенного биометрическим паролем.

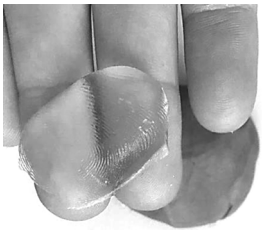

Рис. 1. На изображении расположен желатиновый слепок отпечатка пальца, позволивший разблокировать телефонное устройство

Таким образом, проанализировав всю информацию и проведя научно-практический эксперимент, можно сделать вывод о том, что биометрический способ защиты информации на телефонных устройствах является ненадеженым, так как в повседневной жизни каждый из нас имеет возможность обойти биометрическую систему защиты, используя неправомерные способы входа. В связи с этим считаем необходимым совершенствовать систему защиты телефонных устройств с помощью отпечатков пальцев и повышать качество сенсоров, считывающих информацию узора с пальца руки. Однако все же не рекомендуется хранить конфиденциальную информацию на личных цифровых устройствах.

Об участии специалиста в изъятии электронных носителей информации

М. В. Старичков,
начальник кафедры,
кандидат юридических наук, доцент
(Восточно-Сибирский институт МВД России)

В статье рассматриваются правовые и организационные вопросы участия специалиста в изъятии электронных носителей информации в ходе производства следственных действий.

Электронные носители информации, участие специалиста, расследование компьютерных преступлений, обыск, выемка.

Повсеместное распространение компьютерных технологий, внедрение их во все сферы человеческой деятельности привело к тому, что электронные носители информации все чаще выступают в качестве объектов, содержащих сведения о преступлении.

Изъятие таких носителей в качестве вещественных доказательств нередко затрагивает интересы потерпевших и третьих лиц, а иногда может сделать невозможной дальнейшую работу организации. Так, например, происходит, если необходимо изъять информацию о движении денежных средств клиентов кредитно-финансовых учреждений, о соединениях абонентов сотовых телефонных компаний и др. В подобных ситуациях существует единственный приемлемый способ – снятие копии информации на другие электронные носители. Хотя в криминалистике аналогичные приемы используются уже достаточно давно, например при снятии отпечатков пальцев с предметов или изготовлении слепков следов, оставленных на грунте, законодатель решил прямо указать на такую возможность. Разработчики законопроекта ставили своей целью обеспечить возможность продолжения деятельности организаций и предпринимателей в случае изъятия электронных носителей информации. В результате Федеральный закон от 28 июля 2012 г. № 143-ФЗ УПК РФ был дополнен нормами, вводящими само понятие электронных носителей информации и регулирующими производство следственных действий, в результате которых происходит их изъятие.

Изъятие производится, как правило, в результате таких следственных действий, как осмотр (ст.ст. 176, 177 УПК РФ), обыск (ст. 182 УПК РФ), выемка (ст. 183 УПК РФ). Общие принципы копирования содержащейся на изымаемых электронных носителях инфор-

мации регулируются ч. 2.1 ст. 82 УПК РФ и предусматривают участие в его производстве законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации либо их представителей, специалиста и понятых. При этом УПК РФ указывает, что снятие копий осуществляется в подразделении органа предварительного расследования или в суде. Очевидно, что данное положение применимо не во всех случаях. Например, даже краткосрочное изъятие сервера тарификации сотового оператора затрагивает интересы многих тысяч лиц и влечет убытки, превосходящие ущерб, причиненный расследуемым преступлением.

Специальные нормы, регулирующие производство обыска (ч. 9.1 ст. 182 УПК РФ) и выемки (ч. 3.1 ст. 183 УПК РФ), не определяют место производства копирования. Исходя из общего принципа их построения, копирование должно осуществляться по месту производства следственного действия. Однако если в случае осмотра (и иных следственных действий) специалист необходим только для снятия копий, изъятие электронных носителей информации в ходе обыска или выемки в любом случае должно производиться с его участием. Заметим, что к электронным носителям информации относятся не только накопители на жестких магнитных дисках, входящие в состав системных блоков персональных компьютеров и ноутбуков, лазерные диски, флэш-накопители, карты памяти, но также цифровые фотовидеокамеры и, самое главное, сотовые телефоны, смартфоны и т. п.[1]

В настоящее время подавляющее большинство населения владеет мобильными телекоммуникационными устройствами, а поскольку в их памяти могут содержаться сведения о контактах лица, его переписка, в т. ч. в социальных сетях, фотографии и видеофрагменты, имеющие отношение к расследуемому преступлению, то такие предметы следователь просто обязан будет изъять[2]. Но недостаточное количество сотрудников экспертно-криминалистических подразделений, а тем более имеющих допуск на производство судебных компьютерных экспертиз, ставит под сомнение выполнимость указанных норм, на что нами ранее обращалось внимание[3].

---

[1] *Старичков М.В.* Электронные носители как источники криминалистически значимой информации / М.В. Старичков, В.А. Антонов // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Иркутск: ФГКОУ ВПО Вост.-Сиб. ин-т МВД России, 2013. С. 123–127.

[2] *Грибунов О.П.* Средства сотовой связи как источник криминалистически значимой информации / О. П. Грибунов // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2017. № 4. С. 137–142.

[3] *Старичков М.В.* Особенности изъятия электронных носителей информации / М. В. Старичков // Деятельность правоохранительных органов в современных услови-

На практике такое положение приводит к тому, что изъятие электронных носителей информации в ходе обыска или выемки не всегда производится с участием специалиста[1]. В этом случае и отношение судов к таким доказательствам неоднозначное. Например, апелляционную жалобу адвоката М., действующего в интересах обвиняемого в незаконном перемещении через таможенную границу Таможенного союза в рамках ЕврАзЭС стратегически важных ресурсов в крупном размере (ч. 1 ст. 226.1 УК РФ) гражданина Щ., о незаконности изъятия у него в ходе обыска системного блока персонального компьютера, поскольку данное следственное действие было проведено в нарушении требования ч. 9.1 ст. 182 УПК РФ, без участия специалиста, суд Еврейской автономной области оставил без удовлетворения. Свое решение суд мотивировал тем, что перед началом обыска Щ. был ознакомлен с постановлением суда о производстве обыска в его жилище, и ему было предложено выдать интересующие следствие документы, машинные носители информации, компьютерную технику, а также ценности, добытые преступным путем. Все изъятые в ходе обыска предметы и документы, подробно отраженные в протоколе обыска, были выданы Щ. добровольно. При этом никаких заявлений и ходатайств от участников следственного действия, в т. ч. от Щ., не поступало[2].

Одновременно полученная без участия специалиста распечатка сообщений с интернет-сайта С. от пользователя под логином Л. была признана недопустимым доказательством. Соответственно, были признаны недопустимыми протоколы выемки указанной распечатки и ее осмотра[3].

Таким образом, уголовно-процессуальное законодательство, регулирующее вопросы получения доказательств с электронных носителей информации, нуждается в совершенствовании[4]. Вместе с тем, от лиц, производящих расследование, требуется строгое соблюдение закона и, в частности, привлечение к изъятию в ходе обыска или выемки электронных носителей информации специалиста.

ях: материалы XIX Междунар. науч.-практ. конф. Иркутск: ФГКОУ ВПО ВСИ МВД России. 2014. С. 225–227.

[1] *Васюков В. Ф.* Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / В. Ф. Васюков, А. В. Булыжкин // Российский следователь. 2016. № 6. С. 3–8.

[2] Апелляционное постановление от 16 мая 2017 г. по делу № 22-265/2017 // Архив суда Еврейской автономной области. 2017.

[3] Приговор от 23 декабря 2013 г. по делу № 1-535/2013 // Архив Индустриального районного суда г. Барнаула (Алтайский край). 2013.

[4] *Старичков М.В.* Особенности изъятия электронных носителей информации / М. В. Старичков // Деятельность правоохранительных органов в современных условиях: материалы XIX Междунар. науч.-практ. конф. Иркутск: ФГКОУ ВПО ВСИ МВД России, 2014. С. 225–227.

Актуальные проблемы совершенствования методического обеспечения судебно-экспертной деятельности

Т. В. Толстухина,
заведующая кафедрой,
доктор юридических наук, профессор
(Тульский государственный университет)

А. В. Светличный,
доцент кафедры,
кандидат юридических наук
(Тульский государственный университет)

Д. В. Панарина,
ассистент кафедры
(Тульский государственный университет)

Статья посвящена вопросам совершенствования методического обеспечения экспертной деятельности, ее стандартизации; рассматриваются элементы стандарта судебно-экспертной методики, обозначаются и раскрываются основные требования, которым должны соответствовать судебно-экспертные методики.

Судебная экспертиза, стандартизация, судебно-экспертные методики, методы экспертного исследования.

Выбранная для судебно-экспертной методики система методов и средств исследования объектов должна быть объективной, четко сформулированной, точной и обеспечивать последовательно воспроизводимые результаты.

К структурным элементам стандарта судебно-экспертной методики можно отнести элементы построения, изложения, оформления, содержания и обозначения стандарта.

Следовательно, применяемые методики должны быть общепризнанными и общеизвестными. Такая ситуация может стать реальной при создании и утверждении на соответствующем уровне каталогов экспертных методик. Необходимость стандартизации экспертных методик учеными отмечается уже на протяжении 30 лет[1].

[1] См., напр.: *Волчецкая Т. С.* Криминалистическая ситуалогия. М., 1997. С. 43; *Устинов А. И., Сонис М. А.* О стандартизации методик в судебной экспертизе // Актуаль-

Авторы отметили, что каталогизация (систематизация) экспертных методик по видам и подвидам экспертиз является одной из актуальных задач. Для ее реализации необходима разработка стандартизированной формы изложения. Подобные попытки были предприняты в ЭКЦ МВД России, где были созданы каталоги некоторых стандартизированных методик. Следует иметь в виду, что такие каталоги обязательно должны иметь следователи и судьи. Аналогичной точки зрения придерживался и известный процессуалист В. Д. Арсеньев, с интересом и глубоко изучавший проблемы теории и практики судебной экспертизы[1].

Судебно-экспертные методики специально разрабатываются для исследования каждого вида объекта. В своем большинстве методики разрабатываются головными экспертными учреждениями и публикуются в ведомственных изданиях, поскольку научно-методическое обеспечение производства судебных экспертиз возлагается соответствующими федеральными органами исполнительной власти на государственные судебно-экспертные учреждения (ст. 38 ФЗ ГСЭД). По новым и формирующимся родам (видам) экспертиз методики могут на первом этапе заимствоваться из материнской науки и без надлежащей модификации использоваться для решения простых прямых задач исследования объектов судебной экспертизы. Однако неизбежно практика судебно-экспертной деятельности заставляет модифицировать и оптимизировать такие методики, адаптируя их к специфике судебно-экспертного исследования, а также к возможному изменению законодательства.

Целесообразно дополнить классификацию видов экспертных методик стандартизованной типовой экспертной методикой, содержание которой отвечает обязательным для применения предписаниям стандарта. Необходимо уточнить понятие стандартизованной судебно-экспертной методики, исходя из общеобязательных требований по выполнению содержащихся в ней категорических предписаний, а также набору четких правил и однозначного алгоритма принятия решения экспертом по результатам проведенных исследований, исключающих неоднозначность интерпретации полученных данных и их вольного толкования.

Методики должны быть обеспечены однозначной стандартной инструкцией, необходимыми показателями надежности и валидности применяемых методов. Результаты проверки методик должны быть

ные проблемы теории и практики судебной экспертизы. М., 1989. С. 94.

[1] *Арсеньев В.Д.* Основные документы судебной экспертизы // Вопросы теории судебной экспертизы. М., 1977. С. 5.

опубликованы в научной печати, а методическое обеспечение доступно для ознакомления и рецензирования научным сообществом.

Тем не менее, следует констатировать, что эксперты-психиатры, к сожалению, не имеют разработанных и апробированных методик для решения вопроса: связано ли отставание в психическом развитии с психическим расстройством или же оно связано с педагогической и социальной запущенностью.

Однако расхождение в экспертных методиках, влекущее получение разных результатов при одних и тех же исходных данных и объектах исследования, отдельными недобросовестными участниками процесса может быть использовано в собственных интересах или в интересах представляемых ими лиц. Поэтому отсутствие заинтересованности министерств и ведомств в создании единой судебно-экспертной службы не вполне понятно.

Представители иной точки зрения считают, что такая жесткая регламентация выбора экспертной методики недопустима (или невозможна по тем или иным причинам), и эксперт вправе самостоятельно решать вопрос о выборе методики, исходя из собственных научных познаний и основываясь на общих принципах допустимости научно-технических средств и методов в судопроизводстве. Так, А.Р. Шляхов писал: «Практика показывает, что иногда экспертам приходится разрабатывать новые способы и приемы исследования вещественных доказательств для успешного решения поставленных вопросов, если к моменту назначения экспертизы в распоряжении эксперта нет готовой, достаточно эффективной методики либо существующими методами не удалось решить задачу»[1]. Сторонниками данной точки зрения также являются Р.С. Белкин [2], Е.Р. Россинская[3], чью позицию отчасти разделяем и мы.

В истории России уже были попытки жесткой регламентации судебных экспертных методик. Так, до июня 2006 г. исследования наркотических средств (психотропных, сильнодействующих и ядовитых веществ) в соответствии с постановлением Пленума Верховного Суда Российской Федерации от 27 мая 1998 г. № 9 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» проводились в обязательном порядке по методикам, утвержденным Постоянным комитетом по контролю наркотиков (ПККН). К тому времени ПККН были утверждены методики исследования лишь некоторых веществ из указанных в Перечне наркоти-

---

[1] *Шляхов А.Р.* Судебная экспертиза: организация и проведение. М., 1979. С. 83.

[2] *Белкин Р.С.* Курс криминалистики. М., 2001.

[3] *Россинская Е.Р., Галяшина Е.И., Зинин А.М.* Теория судебной экспертизы. М., 2009.

ческих и психотропных веществ. В связи с этим в ходе судебного разбирательства сторона защиты иногда ставила вопрос о допустимости заключения судебной экспертизы, при проведении которой использовались методики, не утвержденные ПККН.

В дальнейшем постановлением Пленума Верховного Суда РФ от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» было отменено обязательное условие в ограничении использования методик по исследованию контролируемых веществ и средств.

Так, например, В. Н. Карагодин отмечает, что на территории Свердловской области первые случаи изъятия так называемых курительных и ароматизирующих смесей были зафиксированы в ноябре – декабре 2008 г. Но в связи с отсутствием на тот период рекомендованных методик по их исследованию экспертизы по установлению присутствия психоактивных веществ в курительных смесях не проводились. Однако проблема была поставлена перед экспертами, и ее надо было решать. Оперативная информация о применении этих смесей в качестве психоактивных веществ побудила экспертов-химиков к поиску информации о составе подобных смесей в иностранных источниках.

В Европе к этому времени, после появления сообщений о применении синтетических веществ ряда JWH для пропитки растительных смесей якобы из «экзотических травок», многие европейские государства ввели запрет на оборот этих веществ и средств (например, Германия – в январе 2009 г., через месяц после обнаружения факта применения синтетических каннабиноидов, Франция – в феврале 2009 г.). Резкий всплеск случаев изъятия курительных смесей был зафиксирован на территории нашей страны (в Свердловской области в том числе) в августе – сентябре 2009 г., когда поток этих веществ был фактически перенаправлен из европейских стран, запретивших их оборот у себя, в Россию. В течение 2009 г. в иностранных средствах массовой информации и научных журналах стали публиковаться данные о синтетических каннабиноидах и методах их исследования. На основе этих сведений российскими экспертами-химиками самостоятельно стали разрабатываться методики по исследованию синтетических препаратов.

В результате совместной работы правоохранительных органов постановлением Правительства РФ от 31.12.2009 № 1186 несколько синтетических каннабиноидов (25 наименований) и их препараты были отнесены к наркотическим средствам, оборот которых на территории России запрещен. После запрета этих психоактивных веществ ЭКЦ МВД России в целях создания методической базы для производ-

ства экспертиз обобщил опыт отечественных экспертов в информационном письме (исх. № 37/24-1550 от 26.02.2010) «Исследование растительных смесей («спайсов»), содержащих наиболее распространенные синтетические каннабиноиды», где уже были приведены методики исследования указанных веществ, в том числе разработанные и предложенные экспертами территориальных химических лабораторий.

Позднее, в августе 2010 г. на основе данных методик ЭКУ Департамента ФСКН России (в сотрудничестве с ЭКЦ МВД России) были выпущены методические рекомендации «Экспертное исследование курительных смесей, содержащих наиболее распространенные синтетические каннабиноиды». Методические рекомендации были одобрены 30 июля 2010 г. на 24-м заседании Федерального межведомственного координационно-методического совета по судебной экспертизе и экспертным исследованиям для применения в практической деятельности экспертно-криминалистических подразделений государственных судебно-экспертных учреждений федеральных органов исполнительной власти РФ.

Таким образом, с момента появления новых наркотических средств на территории России до выпуска утвержденной методики по их исследованию прошло более полутора лет. И все это время эксперты выполняли их исследование, исходя из своих профессиональных познаний и опыта, используя информацию, полученную из различных научных источников[1].

Нам представляется, что ведущие экспертные учреждения должны оперативнее реагировать на появление новых объектов исследования и разрабатывать экспертные методики.

В отдельных чрезвычайных случаях эксперта нельзя лишать права эвристического подхода к решению задачи.

Таким образом, создание единых нормативных основ судебной экспертизы – один из путей оптимизации деятельности по вовлечению в сферу уголовного судопроизводства результатов судебно-экспертной деятельности.

Совершенно очевидно, что совершенствование методического обеспечения экспертной деятельности, ее стандартизация и унификация для различных экспертных учреждений – главный источник повышения качества производства судебных экспертиз, а следовательно, повышения роли судебных экспертиз в процессе доказывания по гражданским и уголовным делам.

---

[1] *Карагодин В.Н.* Пределы самостоятельности судебного эксперта в выборе методики экспертного исследования // Материалы 3-й Международной научно-практической конференции «Теория и практика судебной экспертизы в современных условиях» (г. Москва, 25–26 января 2011 г.). М.: Проспект, 2011. С. 57–61.

К вопросу о доказательственном значении компьютерной информации

О. В. Тушканова
(ЭКЦ МВД России)

В статье рассматривается понятие компьютерной информации, ее значение для процесса доказывания.

Компьютерная информация, компьютерная программа, доказывание.

В процессе выявления, раскрытия и расследования преступлений у сотрудников следственных и оперативных подразделений возникает ряд проблем, связанных с оценкой статуса и доказательственного значения компьютерной информации, расположенной, в том числе, в изымаемых средствах вычислительной техники.

Практически все сотрудники правоохранительных органов являются в настоящее время владельцами различных средств вычислительной техники[1] (компьютеров, смартфонов, планшетов, флеш-накопителей, автомобильных видеорегистраторов, навигаторов и т. п.) и на интуитивном уровне понимают, что информация, расположенная в этих объектах, является компьютерной. При этом физическая сущность данного понятия остается для них «за кадром».

Законодательное определение компьютерной информации дано в Примечании 1 к ст. 272 УК РФ, в котором указано, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Данное определение нужно признать крайне неудачным, потому что ни «бугорки» и «впадинки» на оптических носителях информации, ни направление вектора намагниченности домена на пластинах накопителей на жестких магнитных дисках, ни уровни заряда в ячейках микросхем флеш-памяти никакого отношения к форме электрических сигналов не имеют.

Добавление прилагательного «компьютерная» к понятию «информация» ничего не изменило в ее сущности, а лишь указа-

[1] Средство вычислительной техники (далее – СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

ло на иную форму ее представления. К отображению информации на привычных «бумажных» носителях, фотопленках, грампластинках, кассетах и проч. добавились отображения на машинных носителях информации в цифровой форме (закодированной в виде «0» и «1» – наличием/отсутствием отверстий в перфокартах и перфолентах, «бугорками» и «впадинками» на оптических накопителях и т. д.). Такая форма представления информации разработана для удобства обработки больших объемов информации с использованием специально созданных для этого устройств (осуществляющих кодирование, запись, воспроизведение, обработку и т. д. компьютерной информации).

Поэтому, с точки зрения криминалистики, компьютерной информацией можно назвать информацию, представленную в цифровой форме, необходимой для ее хранения, обработки и передачи средствами вычислительной техники.

Ключом к уяснению доказательственного значения компьютерной информации является определение ее статуса по отношению к материальному миру. До сих пор многие юристы считают ее самостоятельным материальным объектом, существующим в средстве вычислительной техники. Так, под компьютерной программой ими понимается некий самостоятельный материальный объект, который производит различные манипуляции с данными (создает, обрабатывает, удаляет и др.).

В то же время любой технический специалист понимает, что программа – это набор инструкций, в соответствии с которыми средство вычислительной техники оперирует с данными (сведениями, описывающими свойства материального мира). Как работа двигателя внутреннего сгорания обусловлена законами физики, так работа компьютера осуществляется в соответствии с наборами инструкций (командами по чтению, записи, передаче, обработке данных, собранными в программы).

Понимание этого важно для правильного применения к компьютерной информации таких криминалистических понятий, как идентификация, классификация и диагностика.

Сведения о действиях пользователя определяются логическим уровнем восприятия информации. Образование цифровых следов происходит путем создания, изменения, удаления информации на машинном носителе и отражается в системных, временных, специализированных файлах, свойствах и метаданных файлов данных. Наличие такой информации, возможности доступа к ней и интерпретации зависят как от разработчиков операционных систем, создателей прикладного программного обеспечения, так и от конкрет-

ной реализации аппаратной части устройства. Так, если разработчик программного обеспечения не предусмотрел фиксации сведений о действиях, производимых игроком в процессе игры на игровом автомате, получить эту информацию из запоминающих устройств автомата невозможно.

Особенности записи данных (формирования «0» и «1» на машинных носителях) обусловлены физическими свойствами используемого оборудования и не имеют отношения к идентификационным свойствам пользователя конкретного устройства.

Идентификация объектов по информации, представленной в цифровой форме, проводится, если в файлах запечатлены уникальные свойства объекта (внешность и/или голос человека, особенности объектива фото/видеокамеры, загрязнения на стекле сканера и т. д.). Однако в файлах не отображаются идентификационные свойства лица их создававшего. Более того в создании файла, его изменении, печати, копировании, удалении могут участвовать разные лица. Соответственно эксперт не может оценить относимость найденной им информации как к событию преступления, так и к его участникам, он просто констатирует наличие информации, удовлетворяющей каким-либо критериям, а также сведений о ее обработке (создании, изменении, передаче и т. д.).

Поэтому информация, извлекаемая из средства вычислительной техники, должна быть тщательно изучена лицом, назначившим экспертизу/исследование. Ее необходимо оценить как с точки зрения относимости к расследуемому событию, так и к лицу, у которого было изъято такое средство, в том числе путем сопоставления с другими доказательствами.

Тактика получения и анализа информации, передаваемой в сетях связи с использованием технологии оконечного шифрования, при расследовании преступлений террористического характера

М. А. Ульянова,
студентка
(МГТУ им. Н.Э. Баумана)

Постоянное усложнение технологий передачи данных позволяет создавать все более и более защищенные сервисы информационного обмена. Однако подобные процессы обеспечивают повышенный уровень безопасности не только коммерческим компаниям и рядовым пользователям, но и преступникам. И если первые обращаются за услугами анонимизации своей активности в сети Интернет и шифрованию информации в целях защиты от различных преступных посягательств, то вторая категория пользователей применяет их в ровно противоположных целях – для получения несанкционированного доступа к охраняемым сведениям и иной противоправной деятельности.

Шифрование, терроризм, мобильные устройства, мессенджер, «человек посередине», оперативно-розыскные мероприятия.

Особенную важность в последнее время приобретает предупреждение террористических актов, инициаторы которых широко используют мобильные средства связи для координации своих действий и привлечения новых сторонников[1]. Наиболее надежным и эффективным средством осуществления деятельности данных лиц являются мессенджеры, представляющие собой программные продукты (приложения) и позволяющие клиентам обмениваться сообщениями в режиме реального времени с использованием сети Интернет.

Так, в 2017 г. ФСБ России при проведении оперативно-розыскных мероприятий (ОРМ) по выявлению территориальных группировок международных террористических организаций (МТО) обнаружила факт повсеместного использования их членами интер-

[1] *Долинко В.И.* Актуальные вопросы управления в социально-экономических системах: сборник материалов всероссийского научного семинара. М., 2015.

нет-мессенджеров, применяемых для осуществления конспиративной связи. По данным ФСБ России, самым популярным в террористической среде стал мессенджер «Telegram», обеспечивающий возможность конфиденциального общения в секретных чатах с применением эффективных алгоритмов шифрования данных. В пресс-службе ведомства сообщалось, что упомянутый сервис был использован при подготовке теракта 3 апреля 2017 г. в метрополитене г. Санкт-Петербурга[1].

Привлекательность мессенджера «Telegram» для лиц, стремящихся скрыть свою личную онлайн-переписку, заключается в технической политике обеспечения конфиденциальности. Диалоги могут вестись как в открытых, так и в закрытых («секретных») чатах. В первом случае шифрующие ключи имеются на сервере компании «Telegram», соответственно, их получение возможно путем направления официального запроса уполномоченными органами в соответствии с законодательством. Однако секретные чаты созданы с использованием технологии оконечного шифрования («end-to-end»), при котором ключи генерируются на устройствах пользователей. При этом со стороны сервера доступ к ключам отсутствует, соответственно, получить необходимую информацию в незашифрованном виде не представляется возможным, на что и ссылался создатель мессенджера Павел Дуров, комментируя блокировку «Telegram» в апреле 2018 г. Вместе с тем, альтернативные мессенджеры WhatsApp и Viber используют шифрование всех переписок.

При отсутствии начальных сведений о контактирующих лицах (пользователях) задача действительно технически неосуществима на данный момент. Однако в случае установления списка контактов на изъятом устройстве лица, подозреваемого в принадлежности к террористической группировке, можно выявить ее потенциальных участников и получить доступ к их переписке между собой и с задержанным лицом при помощи алгоритма вероятностной идентификации пользователей в сети и атаки вида «человек посередине».

Предположим, что в результате ОРМ произошло задержание члена террористической группировки, в ходе которого у данного лица было изъято мобильное устройство с каким-либо установленным мессенджером, использующим схему шифрования на основе

---

[1] ФСБ России фиксирует тотальное использование членами законспирированных ячеек международных террористических организаций интернет-мессенджеров для осуществления конспиративной связи между собой и своими кураторами из-за границы // Подробная информация: Федеральная служба безопасности. [М.], 1999–2018. URL: http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10438169%40fsbMessage.html (дата обращения: 29.04.2018).

алгоритма Диффи-Хеллмана. В настоящей следственной ситуации алгоритм действий может быть следующим.

Получение доступа к устройству при наличии начальных элементов защиты (паролей, PIN-кодов) при помощи программно-аппаратных комплексов UFED CHINEX или «Мобильный криминалист».[1]

Извлечение данных (диалогов) из установленного клиента мессенджера, установление списка проверяемых пользователей.

Инициация направления запроса в компанию, являющуюся собственником мессенджера, для получения имеющихся сведений о пользователе (уровень активности, IP-адреса, информация об устройстве, с которого осуществляется вход, местоположение и пр.).

Построение вероятностных связей между пользователями (создание социального графа), установление данных соединения.

Настоящий этап является одним из определяющих в описываемом алгоритме. Канал связи, составляемый с участием пользователя, устройство которого находится на исследовании, в рассматриваемом случае становится дополнительным средством установления данных клиентов мессенджера, с которыми задержанным ранее велась переписка. Так как технология оконечного шифрования предусматривает частую смену ключей (обычно с периодичностью от 10 минут до 1 часа), то именно указанная тактика позволит получить максимальное количество информации.

Далее, основываясь на статистических характеристиках передаваемого с обеих сторон трафика, проводится их анализ и рассчитывается объем передаваемых в единицу времени данных. На протяжении сеанса связи скорость передаваемых пользователями данных изменяется, что образует функцию, которую с большой вероятностью можно считать уникальной характеристикой данного соединения среди всей совокупности остальных сеансов связи.[2] Подобные действия повторяются с массивом данных передачи трафика других пользователей, выявляются связи.

Контроль за каналом связи подозреваемых может быть установлен при помощи программных продуктов и модификаций (настрой-

---

[1] *Грибунов О.П.* Средства сотовой связи как источник криминалистически значимой информации // Вестник Восточно-Сибирского института МВД России. 2017. № 4 (83). URL: https:// cyberleninka.ru/article/n/sredstva-sotovoy-svyazi-kak-istochnik-kriminalisticheski-znachimoy – informatsii (дата обращения: 29.04.2018).

[2] *Тюрин К. А., Болдырихин Н.В.* Алгоритм вероятностной идентификации пользователей сети // Молодой исследователь Дона. 2016. № 2. URL: https://cyberleninka.ru/article/n/algoritm-veroyatnostnoy-identifikatsii-polzovateley-seti (дата обращения: 29.04.2018).

ка сетевого моста, root-управления шлюзом и др.) и программно-аппаратных средств перехвата и анализа трафика. К последним относятся внедряемые в настоящее время системы технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ), в данной ситуации – СОРМ-3, предназначенный для анализа соединений сети Интернет. Такими системами являются «Яхонт» и «Январь». К указанной категории также принадлежат технологии DPI (англ. Deep Packet Inspection), позволяющие осуществлять глубокий анализ проходящих в сети пакетов.

Реализация атаки «человек посередине» (англ. Man-in-the-Middle, MITM), заключающейся во внедрении клиента-посредника между двумя коммуницирующими пользователями. Основанием применения указанного типа атаки является специфика технологии оконечного шифрования: несмотря на то, что ключ генерируется на устройстве, его передача происходит по открытому каналу связи (чаще всего). Клиент мессенджера задержанного связывается с клиентом подозреваемого, он отвечает, а посредник перехватывает сообщения с ключом и заменяет его. Таким образом, переписка подозреваемых из определенного круга пользователей теоретически может быть расшифрована сторонним наблюдателем в рамках проведения получения компьютерной информации (ОРМ, введенное ФЗ № 374 от 6 июля 2016 г.)[1].

Фиксация сведений, отражение их в заключении эксперта (специалиста).

Описанная тактика теоретически может помочь осуществлять получение информации об объектах оперативного интереса, формировать «электронное досье» предполагаемых преступников, обнаруживать скрытые связи с другими пользователями и преступными деяниями; возможно выявление террористических группировок, уровня их организованности и технического оснащения, определять выполняемые ими роли, причастность подозреваемых к определенным событиям. Описанная схема может создать техническую основу прогнозирования терактов и их предупреждения путем выявления электронных следов с определенными параметрами, анализ которых указывает на вероятность подготовки, организации и совершения терактов и иных преступлений.

---

[1] *Осипенко А.Л.* Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. 2016. № 3. URL: https://cyberleninka.ru/article/n/novoe-operativno-rozysknoe-meropriyatie-poluchenie-kompyuternoy-informatsii-soderzhanie-i-osnovy-osuschestvleniya (дата обращения: 29.04.2018).

Проблемы использования информационно-аналитических учетов при расследовании незаконного оборота наркотических средств, совершаемого с использованием информационно-телекоммуникационных технологий

Л. Е. Чистова,
доцент кафедры,
кандидат юридических наук
(Московский университет МВД России
им. В. Я. Кикотя)

В статье обращается внимание на проблемы, возникающие в процессе расследования преступлений, связанных с незаконным оборотом наркотических средств при использовании информационно-аналитических учетов. Предлагается авторское решение данных проблем.

Незаконный оборот наркотиков; информационно-аналитические учеты, расследование преступлений.

Расследование незаконного оборота наркотических средств невозможно без использования соответствующих учетов. Что же касается информационно-аналитических учетов, то для расследования уголовных дел рассматриваемой категории сведений, содержащихся в них, уже недостаточно. Связано это с тем, что преступления данного вида все чаще совершаются в виртуальном пространстве и с использованием различных электронных средств связи и Интернета. В связи с этим действия преступников носят бесконтактный характер. Это относится не только к сбыту наркотических средств, когда приобретатель заказывает их через интернет-магазины, оплачивает через электронные терминалы и получает через закладки, не вступая в контакт со сбытчиками. Все действия членов организованных преступных формирований от получения указаний от вышестоящих руководителей до общения внутри конкретного звена осуществляются с помощью современных средств связи: радиотелефонов, пейджеров, малогабаритных радиостанций и другой новейшей электронной техники. Поэтому традиционных следов остается все меньше, и для выявления, изобличения преступников и выяснения иных обстоятельств незаконного оборота наркотических средств все большее значение имеют компьютерные и иные информационные следы.

В связи с этим мы согласны с мнением С. С. Овчинского о том, что наряду с традиционным информационным обеспечением необходим «переход от автоматизированных учетов и информационно-поисковых систем к системам нового поколения, основанным на мультимедийных компьютерных технологиях»[1].

Объектами таких учетов, как нам представляется, могут быть голос преступников, их фотоизображения, электронные сообщения, схемы деятельности преступных формирований. Самым распространенным объектом такого учета и самым веским впоследствии доказательством изобличении наркопреступников является их голос.

Поскольку образцы голосов лиц, связанных с незаконными действиями в сфере незаконного оборота наркотиков, получают из материалов прослушивания телефонных переговоров, по ним можно выяснить роли участников переговоров по их содержанию, интонации и передаваемой информации, в т. ч. указаний, касающихся совершения определенных действий конкретными лицами. В связи с этим можно вычислить и определить руководителей преступных формирований. Это очень важный момент, потому что, как правило, именно руководителей очень сложно привлечь к уголовной ответственности в силу того, что в преступной цепочке они очень далеко отстоят от исполнителей и иных лиц, входящих в низшие звенья того или иного формирования, и эти участники преступной деятельности в лицо их не знают, сами они в незаконных действиях с наркотическими средствами непосредственного участия не принимают и, соответственно, никаких традиционных следов в связи с этим не оставляют. Поэтому таким лицам довольно часто удается уходить от уголовной ответственности.

В связи с этим совершенно верно замечание П. П. Ищенко и Е. П. Ищенко: «...количество выявленных преступлений, предусмотренных ст. 210 УК РФ, явно не соответствует уровню организованной современной наркопреступности, а количество судебных приговоров с этой квалификацией – и того меньше. Может создаться впечатление, что преступным наркобизнесом занимаются чуть ли не одиночки»[2].

---

[1] *Овчинский С. С.* Оперативно-розыскная информация. Теоретические основы информационно-прогностического обеспечения оперативно-розыскной и профилактической деятельности органов внутренних дел по борьбе с организованной преступностью. М., 2017. С. 329.

[2] *Ищенко Е. П., Ищенко П. П.* Современные компьютерные технологии в борьбе с организованной наркопреступностью // LEX RUSSICA (Научные труды МГЮА). 2012. № 1. С. 104.

При таких обстоятельствах изобличить руководителей преступных формирований в их причастности к незаконному обороту наркотических средств возможно на основании отождествления его по голосу. Следует заметить, что правоохранительные органы принимают меры к созданию банка данных таких голосов. Например, в «Следственном комитете при МВД России такие сведения аккумулируются в Специализированной территориально распределительной автоматизированной системе органов предварительного следствия и Едином межведомственном банке данных "Невод"»[1].

На наш взгляд, следует также систематизировать голоса лиц, в отношении которых уголовное преследование за незаконный оборот рассматриваемых средств прекращено либо за недоказанностью их участия в таком обороте, либо по иным причинам. Поскольку такие лица, как правило, продолжают свою преступную деятельность в этой сфере и поэтому рано или поздно они все равно попадают в поле зрения правоохранительных органов. В таких случаях фонограмма с записью его голоса может быть использована при его изобличении.

Как нам представляется, учитывать таких лиц следует не только по голосу, но и в виде видеоизображений. Такая необходимость заключается в том, что подобные лица, в зависимости от того, какие конкретно функции в составе преступного формирования выполняют, могут контактировать с другими лицами, не связанными с незаконным оборотом наркотических средств. Например, при приобретении прекурсоров с химических предприятий, якобы для учебных заведений, для незаконного производства синтетических наркотиков или совершать иные действия некриминального характера в целях обеспечения бесперебойного функционирования незаконного оборота таких средств. Поэтому должностные лица, отпускавшие им химические вещества, могут запомнить их приметы и при необходимости оказать содействие правоохранительным органам в установлении причастности к незаконным действиям с этими средствами. Обращение преступников в предприятия химической, сельскохозяйственной и иной промышленности для приобретения определенных прекурсоров происходит довольно часто в тех случаях, если они занимаются изготовлением синтетических наркотиков. Поэтому в тех случаях, когда у сотрудников правоохранительных органов не имеется ни записей голоса лиц, заподозренных в незаконном обороте наркотических средств, ни видеоизображений, следует составлять их субъективный портрет с целью последующего установления личности такого лица.

---

[1] *Ищенко Е. П., Ищенко П. П.* Указ. соч. С. 108.

Помимо того, большая часть прекурсоров, особенно для изготовления амфетамина, поступает в нашу страну контрабандным путем из Китая. «При этом наркодельцы используют огромные возможности развитой химической и фармацевтической промышленности Китая для вывода больших количеств химических веществ»[1].

Поскольку незаконным перемещением прекурсоров занимаются конкретные постоянные лица, в обязанности которых входит осуществление именно этих незаконных действий в структуре преступной цепочки по незаконному обороту наркотических средств, то пересекать государственную границу нашей страны им приходится довольно часто. Мы согласны с Ищенко Е. П. и Ищенко П. П., что также можно создать учет таких лиц по опыту полиции ФРГ. Суть сбора информации о таких лицах заключается в том, что персонифицированные данные, собранные в ходе проверок людей на границе или на контрольных пунктах, обрабатываются, а затем с помощью растрового метода, который представляет собой автоматизированный поиск неизвестных преступников путем электронной обработки различных информационных массивов персональных данных, осуществляется компьютерная обработка данных по поисковому портрету предполагаемого преступника. «В результате обработки баз персональных данных с помощью специальной компьютерной программы из огромного информационного массива выбираются те субъекты, которые соответствуют составленному растру (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»[2].

Перевозят контрабандным путем наркотические средства и мигранты – выходцы из бывших республик Средней Азии. Как нам представляется, следует вести учет лиц, наиболее часто пересекающих Государственную границу России, т. к. именно они могут быть причастны к незаконному обороту этих средств. Причем учет таких лиц возможен как по видеоизображениям, так и по голосу и почерку. Методика идентификации говорящего по голосу и речи на таджикском, узбекском, цыганском и азербайджанском языках была разработана еще ФСКН России[3] и успешно использовалась в расследовании незаконного оборота наркотических средств.

---

[1] *Комиссина И.Н.* Наркоситуация в Китае: последствия для России // Проблемы национальной стратегии. 2014. № 1 (22). С. 101.

[2] *Ищенко Е. П., Ищенко П. П.*. Указ. соч. С. 110–111.

[3] *Ищенко Е. П., Ищенко П. П.* Указ. соч. С. 106.

Как справедливо отмечается в криминалистической литературе, преступники по делам рассматриваемой нами категории все чаще используют для общения между собой ICQ, Skype, Telegram, Viber, Whatsapp. Несмотря на то, что текстовые сообщения, передаваемые через эти средства связи, краткие, как нам представляется, их учет будет способствовать, с учетом накопленных таких сообщений, во-первых, идентифицировать автора. В связи с этим правы П. П. Ищенко и Е. П. Ищенко в том, что «отсутствие в передаваемых сообщениях следов голоса и речи не позволит использовать судебную фоноскопическую экспертизу»[1]. Однако, как отмечает П. П. Ищенко, в его практике «осуществлялась идентификация автора кратких текстовых сообщений, переданных при помощи мессенджера в сети Интернет путем проведения судебной авторовед-ческой экспертизы»[2]. Таким образом, если будет вестись учет таких сообщений, то по тону передаваемых сообщений, во-первых, можно будет установить организатора преступного формирования и иных участников, выполняющих функции перевозчиков, в т. ч. и контрабандистов наркотических средств, их изготовителей, хранителей, курьеров и т. д. Во-вторых, можно проследить схему преступных действий членов этого формирования.

Такая информация поможет оперативным сотрудникам спланировать свои оперативно-разыскные мероприятия для выявления обстоятельств незаконного оборота наркотических средств. А впоследствии, во взаимодействии со следователем, спланировать задержание преступников с поличным и провести иные следственные действия в целях их изобличения. В связи с этим мы полностью согласны с С. С. Овчинским, считающим, что автоматизация таких учетов «позволит поднять оперативно-розыскные и следственные мероприятия на качественно новый уровень»[3].

---

[1] *Ищенко П. П., Ищенко Е. П.* Эволюция организованной преступности в цифровую эпоху // Библиотека криминалиста. Научный журнал. № 6 (29). 2016. С. 227.

[2] *Ищенко П.П., Ищенко Е.П.* Указ. соч. С. 227.

[3] *Овчинский С. С.* Оперативно-розыскная информация. Теоретические основы информационно-прогностического обеспечения оперативно-розыскной и профилактической деятельности органов внутренних дел по борьбе с организованной преступностью. М., 2017. 2-е изд., доп. С. 330.

Актуальные перспективы борьбы с мошенничествами, совершаемыми с использованием средств мобильной связи

А. А. Шаевич,
доцент кафедры,
кандидат юридических наук, доцент
(Восточно-Сибирский институт МВД России)

А. А. Рудых,
(ГУ МВД России по Иркутской области)
В.А. РОДИВИЛИНА,
старший преподаватель,
кандидат юридических наук
(Восточно-Сибирский институт МВД России)

В. А. Родивилина,
старший преподаватель,
кандидат юридических наук
(Восточно-Сибирский институт МВД России)

Авторами дается краткая характеристика современного состояния борьбы с мошенничествами, совершаемыми с использованием средств мобильной связи. Рассматриваются изменения законодательства, регламентирующие деятельность правоохранительных органов и операторов связи в области оказания услуг, способные оказать значительное влияние на борьбу с подобными преступлениями.

Телефонные мошенничества, профилактика, УИС, средства мобильной связи.

В настоящее время все больше традиционных составов преступлений, направленных против собственности граждан, совершаются с использованием информационно-телекоммуникационных технологий. Наиболее распространенным видом преступлений против собственности в телекоммуникационной среде остается телефонное мошенничество, которое, несмотря на многочисленные предупреждения, повышающуюся грамотность и осторожность пользователей мобильных телефонов, продолжает лавинообразно набирать массу. Сложившаяся на данный момент обстановка в этой области является крайне неутешительной. Отмечается

постоянный рост мошенничеств, совершаемых с использованием средств мобильной связи, и это при том, что данный вид преступлений относят к латентным, поскольку по различным причинам достаточно часто о подобных преступлениях в полицию не заявляют. Различным случаям обмана граждан по телефону, совершенного с целью получения от них денежных средств, посвящены многочисленные статьи или заметки в новостных лентах. Активно рассматриваются различные аспекты раскрытия и расследования, проблемы уголовно-правовой квалификации и т. п. и в соответствующей специальной литературе. Позволим себе достаточно большую цитату одной из таких публикаций, в которой, может быть резковато, но абсолютно точно отражена проблема: «... мошенники, совершающие преступления, связанные с использованием средств сотовой связи, практически ежедневно изобретают новые конструкции навязывания индивиду убеждений, согласно которым последний послушно вынужден расставаться со своими денежными средствами в пользу преступников, которые пользуются в своей незаконной деятельности несовершенством российского законодательства, новейшими достижениями науки и техники, низкими интеллектуальными способностями обманываемых людей, слабыми оперативными позициями сотрудников оперативных подразделений органов внутренних дел»[1].

Кроме проблем, обозначенных выше, озабоченность вызывает тот факт, что немалая доля подобных преступлений совершается лицами, отбывающими уголовное наказание в местах лишения свободы. Подобное обстоятельство затрудняет предупреждение и раскрытие преступлений этого вида. По замечанию практических работников, дистанционное мошенничество из мест лишения свободы становится постоянной криминальной формой изъятия денежных средств у граждан России[2].

И это при том, что мобильные телефоны относятся к числу предметов, которыми запрещено владеть осужденным, а для пресечения фактов незаконного владения запрещенными предметами администрация учреждения имеет право производить досмотр находящихся на территории исправительного учреждения лиц,

---

[1] *Горбанев В.М.* Правовая регламентация противодействия мошенничествам, связанным с использованием средств сотовой связи // Уголовная политика и культура противодействия преступности: материалы Международной научно-практической конференции. Краснодарский университет МВД России,. 2016. С. 167.

[2] *Литвинов Н. Д., Федоров А.Н.* Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. № 12 (32). С. 72.

их вещей, изымать запрещенные вещи и документы, производить обыски как самих осужденных, так и занимаемых ими помещений. Однако у осужденных мобильные телефоны имеются в количестве, позволяющем заниматься «мобильным мошенничеством». Существуют различные способы передачи телефонов осужденным, не будем останавливаться на их рассмотрении, но, как справедливо отмечают Н. Д. Литвинов, А. Н. Федоров, «поступление в учреждения мобильных телефонов и возможность пользования ими во многом – следствие неисполнения сотрудниками своих профессиональных обязанностей»[1], что, в свою очередь, позволяет вспомнить о принципе наступательности в выявлении и расследовании преступлений[2].

Кроме того, необходимо упомянуть еще и о том, что покинув места лишения свободы, многие осужденные, занимавшиеся совершением мошеннических действий с помощью средств мобильной связи, не бросают данное направление преступной деятельности. А осведомленность об основных принципах функционирования систем сотовой связи и основных методах работы по поиску лиц, совершивших преступления с использованием мобильных телефонов, закономерно ведет к тому, что преступники принимают определенные меры к сокрытию следов преступления.

Это не только сокрытие личных данных путем использования сим-карт, зарегистрированных на другое лицо и т. п., но и действия, направленные на то, чтобы навести сотрудников правоохранительных органов на ложный след. Так, проведенные нами опросы лиц, занимающихся раскрытием и расследованием преступлений данной категории, вскрыли информацию, которую, по нашему мнению, необходимо учитывать. Зная о том, что правоохранительные органы с помощью биллинга мобильного телефона могут установить примерное место (с определенной погрешностью, зависящей от особенностей местности, а также количества и взаимного расположения станций сотовой связи на определенной территории), откуда осуществлялись сеансы связи или производилась рассылка сообщений, преступниками предпринимаются соответствующие контрмеры. Чаще всего для осуществления звонков и отправки сообщений преступники могут выехать в другие населенные пункты, расположенные за несколько десятков или даже сотен километров. Кроме того,

---

[1] *Там же.* С. 71.

[2] *Гармаев Ю. П.* Принцип наступательности в выявлении и расследовании преступлений // Российский следователь. 2016. № 2. С. 6–12.

известны случаи, когда преступниками подобные действия осуществлялись из автомобиля, максимально близко подъезжавшего к местам отбывания наказания, тем самым провоцируя проверки на территории учреждения ФСИН и поиск преступника среди находящихся там осужденных.

Определенные активные профилактические мероприятия, в том числе использование оборудования, устраняющего техническую возможность осуществления телефонных соединений с территории исправительных колоний, изменяют ситуацию. Однако использование так называемых «глушилок» сопряжено с определенными сложностями, связанными с помехами в работе сотовой связи и даже ее полного блокирования в зданиях, находящихся за пределами территории исправительного учреждения, и как следствие – нарушение прав граждан. Таким образом, использование подобных технических средств не является «панацеей» и необходимо задействовать другие инструменты.

К основным причинам и условиям, способствующим противоправной деятельности, следует отнести доступность «анонимных» средств коммуникации и инструментов перевода и обналичивания денежных средств. Большинство преступлений, совершаемых дистанционно, в том числе мошенничеств, краж, вымогательств, реализуются преступниками при помощи цифровых устройств, находящихся у них в пользовании, и идентификационных модулей (сим-карт), оформленных на третьих лиц, либо на вымышленные данные, а также вообще не оформленных в установленном порядке. Таким образом, одним из наиболее эффективных способов борьбы с подобными видами преступлений является своевременное отключение от услуг связи абонентов, использующих незарегистрированные или зарегистрированные на других лиц сим-карты.

В связи с этим стоит отметить недавние изменения законодательства, регламентирующие деятельность правоохранительных органов и операторов связи в области оказания услуг связи. Одно из таких изменений было внесено постановлением Правительства Российской Федерации от 25 октября 2017 г. № 1295 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам оказания услуг связи», произведен ряд изменений в правила оказания услуг телефонной связи, утвержденных постановлением Правительства Российской Федерации от 9 декабря 2014 г. № 1342 «О порядке оказания услуг телефонной связи». В соответствии с ними теперь при получении соответствующего запроса от органа, осуществляющего оперативно-розыскную деятельность, оператор связи в течение трех рабочих

дней со дня получения обязан направить запрос абоненту с целью подтверждения соответствия его персональных данных сведениям, заявленным в договоре, с указанием даты прекращения оказания услуг связи, в случае неподтверждения соответствия персональных данных. В свою очередь на абонента возлагается обязанность при получении подобного запроса от оператора связи, подтвердить персональные данные. Также оператор связи обязан не менее чем за трое суток до прекращения оказания услуг связи осуществить повторное информирование абонента о дате прекращения оказания услуг связи в случае неподтверждения соответствия персональных данных фактического пользователя сведениям, указанным в договоре.

Аналогичные по содержанию поправки были также внесены в Правила оказания телематических услуг связи, утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи» и правила оказания услуг связи по передаче данных, утвержденных постановлением Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных».

Необходимо отметить Федеральный закон от 29 июля 2017 г. № 245-ФЗ «О внесении изменений в Федеральный закон "О связи"», который вступит в действие с 1 июля 2018 г. Указанным законом внесены ряд изменений и дополнений, в частности четко определяются взаимные права и обязанности оператора связи и абонента в сфере идентификации последнего, а также регламентируется порядок прекращения оказания услуг связи.

Из анализа внесенных изменений в действующее законодательство можно сделать вывод о том, что применение правоохранительными органами и операторами связи представленных возможностей оперативно, системно и последовательно может способствовать эффективному предупреждению дистанционных корыстных преступлений и минимизировать незаконный оборот средств связи. Применительно к вопросу о проблеме дистанционного мошенничества из мест лишения свободы процедура приостановления услуг связи при неподтверждении соответствия личности фактического пользователя сведениям, указанным в абонентском договоре, может быть достаточно эффективно использована при взаимодействии правоохранительных органов с оператором связи с целью ограничения использования услуг связи лицами, отбывающими наказание. Для этого, используя биллинговую информацию о местонахождении телефона (в данном случае

информацию о том, что с определенных номеров осуществляются звонки и отправка коротких сообщений с территории исправительного учреждения (точность зависит от размеров и количества обслуживающих станций в районе), которую абонент не покидает в течение нескольких дней), инициируется проверка соответствия персональных данных и в случае их неподтверждения производится отключение.

Очевидно, что такая мера не сможет решить проблему на все сто процентов, поскольку в течение нескольких дней, пока будут продолжаться описанные процедуры, преступник сможет совершать звонки и рассылку коротких сообщений, но определенный потенциал у нее есть. Определить ее действительную эффективность сможет только практика. Однако наведение порядка в сфере оборота сим-карт и исключение анонимности пользователя должно свести к минимуму совершение как рассматриваемых в данной публикации преступлений, так и ряда других, в способ совершения которых входит использование мобильного телефона.

Использование современных информационных технологий в криминалистической деятельности: проблемы и тенденции

А. С. Шаталов,
профессор кафедры,
доктор юридических наук
(НИУ «Высшая школа экономики»)

В данной статье рассмотрены наиболее актуальные вопросы имплементации в научные ресурсы отечественной криминалистики современных информационных технологий вообще и для повышения эффективности борьбы с преступлениями, совершаемыми с использованием компьютерных и сетевых возможностей, в частности. Борьбу с ними автор считает проблемой международного масштаба, поскольку меры по предотвращению, выявлению, раскрытию и расследованию преступлений такого рода не могут быть результативными лишь на национальном уровне в силу транснационального и трансграничного характера самой сети Интернет. С учетом непрекращающегося увеличения численности ее пользователей, закономерно порождающей их зависимость от информационного сообщества и уязвимость от разного рода киберпосягательств, произведен анализ современного состояния расследования преступлений такого рода и сформулированы рекомендации по повышению эффективности этой деятельности.

Информационные технологии, киберпреступность, компьютерные преступления, криминалистика, криминалистическая методика, расследование преступлений.

Современные информационные технологии занимают в экономике страны особое место, а их эффективное функционирование является одним из важнейших факторов, способствующих решению ключевых задач государственной политики. Важно отметить, что в Российской Федерации они являются наиболее зависимыми от использования импортного программного обеспечения (до 90 % операционных систем и систем управления базами данных). Понимая опасность такого положения дел, ведущие эксперты в области IT-безопасности заявляют о том, что если российской экономикой будет управлять чужой искусственный интеллект, то наша страна

со временем рискует превратиться в цифровую колонию[1]. Во избежание такого развития событий технологическая независимость Российской Федерации в сфере информационных технологий провозглашена основой не только информационной безопасности, но и безопасности государства в целом, в т. ч. от преступных посягательств[2]. Помимо прочего, информационные технологии должны сыграть важную роль в обеспечении дальнейшего поступательного развития отечественной криминалистики. Сейчас стало очевидно, что в ней назрел ряд вопросов, ожидающих своего комплексного решения. Необходимо, в частности, реализовать меры, направленные на разработку и внедрение новых способов предотвращения, выявления, раскрытия и расследования преступлений, совершаемых в киберпространстве.

Распространение компьютерных вирусов, мошенничества с платежными картами, хищения денежных средств с банковских счетов, компьютерной информации, нарушения правил эксплуатации автоматизированных электронных систем, разного рода противоправные действия с использованием криптовалют, блокчейна, искусственного интеллекта – далеко не полный перечень преступлений, совершаемых с их помощью. Данное явление принято называть по-разному: киберпреступностью, компьютерными преступлениями, преступлениями в сфере компьютерных технологий, преступлениями в сфере компьютерной информации и т. д. В литературе, изданной за последнее десятилетие, наиболее часто встречаются два термина: *«киберпреступления»* и *«компьютерные преступления»*. Их можно считать равнозначными, поскольку они используются для обозначения группы одних и тех же общественно-опасных деяний. В криминалистическом аспекте киберпреступления (или компьютерные преступления) – это общественно опасные деяния для подготовки, совершения, сокрытия, а соответственно предотвращения, выявления, раскрытия и расследования которых, применяются разного рода компьютерные технологии и (или) используется информационно-телекоммуникационная сеть Интернет.

Причиной популярности и стремительного роста киберпреступности как некого криминального бизнеса, прежде всего, является его невероятная прибыльность, а сам процесс получения доходов, которые могут превышать миллионы долларов, обычно не ото-

---

[1] *Шадрина Т.* Обогнать, не догоняя // Рос. газ. 2018. № 47 (7510). 5 март.

[2] О развитии информационных технологий в Российской Федерации и мерах поддержки отечественной ИТ-отрасли: постановление Совета Федерации Федерального Собрания РФ от 20 апреля 2016 г. № 154-СФ // Документ опубликован по адресу: www.Consultant.ru/cons/cgi/online.cgi?... (дата обращения: 18.04.2018).

ждествляется с риском разоблачения и наказания, в широком их понимании. Поэтому сама киберпреступность, наряду с экологией, коррупцией и незаконным оборотом наркотиков, фактически стала важнейшей проблемой геополитического масштаба. С наступлением нового века ее решению стало уделяться много внимания как на национальных уровнях, так и в рамках реализации программ международного сотрудничества государственных правоохранительных органов.

Главная криминалистическая особенность киберпреступлений заключается в том, что их предотвращение, выявление, раскрытие и расследование невозможно без использования современных информационных технологий. Соответственно этому возникла необходимость во все бо́льшем внимании к подготовке специалистов для борьбы с такими преступлениями, переподготовке действующих кадров, с тем чтобы эффективно разоблачать преступников, посредством обнаружения, фиксации, изъятия и использования разного рода «электронных» доказательств.

Однако существующая система противодействия преступным посягательствам, совершенным с использованием современных информационных технологий, пока заметно отстает в своем развитии. Сложности обусловлены спецификой совершения преступлений данной разновидности, которая, на наш взгляд, заключается в следующем:

– в доступности (т. е. повсеместной распространенности и относительной дешевизне) компьютерной техники для самых широких слоев населения;

– в весьма «большой» и фактически трансграничной географии совершения преступлений;

– в однозначной досягаемости объекта преступного посягательства (т. е. фактическое расстояние до него не имеет никакого значения);

– в комфортности условий, сопутствующих подготовке и совершению преступлений в киберпространстве (т. е. их подготовка и совершение, реально может осуществляться, практически с любого персонального компьютера, имеющего «выход» во Всемирную паутину).

Сам процесс выявления, раскрытия и предварительного расследования преступлений, совершенных с использованием современных информационных технологий, имеет ряд существенных особенностей. Ошибки, допускаемые при этом следователями и дознавателями, в своем большинстве являются следствием их неудовлетворительной профессиональной подготовки именно для этого сегмента криминалистической деятельности. Одной из наиболее существен-

ных причин низкого качества предварительного расследования преступлений, совершаемых в киберпространстве, в научных публикациях справедливо признается отсутствие качественных методических разработок, в реализации которых были бы в полной мере задействованы современные информационные технологии. В таких условиях объективные сложности обнаружения, фиксации и изъятия криминалистически значимой информации с целью ее дальнейшего использования в качестве доказательств по уголовному делу нередко становятся непреодолимыми. Более того, здесь как нигде высока вероятность того, что те доказательства, что все же были обнаружены, могут быть непреднамеренно изменены и даже утрачены как в результате допущенных ошибок при их фиксации или, например, изъятии, так и в ходе их исследования. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде требует обязательного наличия не только основательной профессиональной подготовки, но и регулярного обновления имеющихся знаний у следователей, дознавателей, оперативных работников и, разумеется, у специалистов и экспертов.

В контексте затронутой проблемы важно отметить, что исследования, посвященные именно получению, обработке, использованию и хранению информации, стали проводиться с середины XX в., т. е. сравнительно недавно. Понадобилось еще примерно пятьдесят лет, для того чтобы информационные технологии получили повсеместное распространение и стали доступными практически всем. Все это привело к появлению преступлений новых видов и, как следствие, к резкому увеличению научных исследований соответствующей тематики. Постепенно стало понятно, что практически все они носят междисциплинарный характер и используют достижения многих наук и в первую очередь криминалистики.

Из общего массива работ, посвященных данной проблематике, можно выделить диссертационные исследования А. В. Касаткина[1] и С. В. Киселева[2], имевшие место в конце 90-х гг. прошлого века, а также диссертации А. А. Шаевича[3], Ю. А. Куриленко[4], А. В. Нариж-

---

[1] *Касаткин А. В.* Тактика собирания и использования компьютерной информации при расследовании преступлений: автореферат дисс. ... канд. юр. наук. М., 1997. 23 с.

[2] *Киселев С. В.* Проблемы расследования компьютерных преступлений: автореферат дисс. ... канд. юр. наук. СПб., 1998. 23 с.

[3] *Шаевич А. А.* Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: автореферат дисс. ... канд. юр. наук. Иркутск., 2007. 24 с.

[4] *Куриленко Ю. А.* Компьютерные технологии как средство повышения эффективности организации правоохранительной деятельности (применительно к деятель-

ного[1], С.А. Ковалева[2], А.А. Косынкина[3], К.В. Костомарова[4] и В.О. Давыдова[5], защищенные в период с 2007 г. по 2013 г. Обращает на себя внимание то обстоятельство, что диссертационные исследования названных авторов (за одним только исключением) проводились не в столичных городах (Москве или Санкт-Петербурге), а в региональных центрах. Причем последнее из них (диссертационное исследование В.О. Давыдова) было защищено в 2013 г., т. е. около пяти лет тому назад. Возникший в последние годы «застой» в исследовательской работе, отчасти был компенсирован публикациями Е.П. Ищенко[6], В.Б. Вехова[7] и некоторых других российских криминалистов, проявивших интерес к данной проблематике. Однако этого оказалось явно недостаточно. Постепенно пришло осознание того, что отсутствие системного и институционального характера в исследовательской работе на этом направлении ощутимо затрудняет борьбу с преступлениями, совершаемыми с использованием постоянно совершенствующихся информационных технологий. Сама же информация выступает объектом преступной деятельности в этой сфере. Ее хищение, изменение, неправомерное использование так или иначе вносит диссонанс в функционирование экономических систем. Более того, в отличие от организованной преступности, коррупции, многих проявлений терроризма и экстремизма, деятельность киберпреступников не согласуется с известными и привычными в обществе моделями поведения. По сути это означает, что она индивидуальна, иррациональна, анонимна и интернациональна, а каждый человек в современном мире, от простого обывателя

ности ОВД по расследованию преступлений): автореферат дисс. ... канд. юр. наук. Саратов., 2008. 23 с.

[1] *Нарижный А.В.* Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: автореферат дисс. ... канд. юр. наук. Краснодар, 2009. 22 с.

[2] *Ковалев С.А.* Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации: автореферат дисс. ... канд. юр. наук. Воронеж, 2011. 22 с.

[3] *Косынкин А.А.* Преодоление противодействия расследованию преступлений в сфере компьютерной информации: автореферат дисс. ... канд. юр. наук. Саратов, 2012. 24 с.

[4] *Костомаров К.В.* Первоначальный этап расследования преступлений, связанных с незаконным доступом к компьютерной информации банков: автореферат дисс. ... канд. юр. наук. Челябинск, 2012. 30 с.

[5] *Давыдов В.О.* Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: автореферат дисс. ... канд. юр. наук. Ростов-на-Дону, 2013. 26 с.

[6] См. например: *Ищенко Е.П.* Виртуальный криминал. Науч.-попул. изд. М.: Проспект, 2015. 232 с.

[7] См. например: *Вехов В.Б.* Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. М., 2016. № 2. С. 10 – 19.

до крупной компании, банка и государства, рискует в любой момент стать жертвой злоумышленников в киберпространстве, постоянно изобретающих новые, сложные и разнообразные схемы мошеннических операций.

Обращает на себя внимание тот факт, что с начала XXI в. и до настоящего времени количество выявленных преступлений в сфере компьютерной информации (ст.ст. 272–274 УК РФ), изменялось практически постоянно. Если в 2001 г. их было зафиксировано около 3,7 тыс., то к 2003 г. их общее количество увеличилось втрое (10,4 тыс.). В последующие годы стал наблюдаться их некоторый количественный спад. В 2015 г., например, было зафиксировано 2 382 таких преступления[1], за совершение которых было осуждено лишь 235 чел. (!). В 2016 г., по данным Судебного департамента при Верховном Суде РФ, эта цифра сократилась до 185 чел.[2]

Причины таких несколько странных количественных расхождений различны. Нам они видятся в том, что абсолютное большинство преступлений в сфере компьютерной информации – латентные. Специалисты правильно утверждают, что до 90 % данных криминальных актов не находят отражения в официальной уголовной статистике[3]. Наиболее распространенная причина такого положения дел, кроется в нежелании практически всех коммерческих предприятий (в т. ч. банков) предавать гласности сведения о похищении у них компьютерной информации и денежных средств путем виртуальных взломов систем их защиты. Объяснение этому простое – они предпочитают дорожить своей репутацией и боятся потерять клиентов, а доказывание фактов совершения таких преступлений – довольно сложное и обременительное занятие.

В США и многих странах европейского континента уже отработана технология поиска киберпреступников. Расходы на розыск каждого из них в среднем составляют немногим более 300 долл.[4]Борьба с киберпреступлениями российскими правоохранительными органами пока оставляет желать лучшего. А если выра-

---

[1] *Михайлова Б. П., Хазова Е.Н.* Особенности противодействия киберпреступности подразделениями уголовного розыска // Состояние преступности в России (за январь – декабрь 2010 г., 2011 г., 2012 г., 2013 г., 2014 г.). ФГУ ГИАЦ МВД РФ. Москва // Режим доступа: www.mvd.ru (дата обращения: 18.04.2018).

[2] Официальный сайт Судебного департамента при ВС РФ // Режим доступа: URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 18.04.2018).

[3] См. например: *Тарасов А.М.* Электронное правительство и информационная безопасность. СПб., 2011. 647 с.

[4] Цит. по: 80 % пользователей не верят, что интернет-преступников можно наказать. Последние новости IT – ITUA.info. URL: http://itua.info/software/28662.html (дата обращения: 18.04.2018).

зится более категорично, то ей особенно некому противостоять. Только 4,5 % следователей обладают более или менее удовлетворительными знаниями по специальности «Информатика и вычислительная техника». Около 72 % из них оценивают свой уровень владения персональным компьютером «как у среднего пользователя»[1]. Здесь есть над чем работать.

Звучит весьма вызывающе и несколько странно, но гораздо эффективнее борьбу с киберпреступлениями в России пока осуществляют несколько агентств, специализирующихся на инициативном расследовании высокотехнологичных преступлений. Они действуют не только в силу собственной заинтересованности в извлечении прибыли, но и по причине наличия у них бо́льших возможностей, знаний и технологического потенциала. Компания «Group-IB», например, за полтора десятилетия своего существования расследовала более тысячи высокотехнологичных преступлений, немалая часть которых являлись особо сложными[2]. Агентство Финансовой и Правовой Безопасности также на этом поприще достигло определенных успехов. В основном за счет использования в работе своих сотрудников не только новейших информационных технологий, но и аккаунтов в социальных сетях[3].

Согласно данным, полученным компанией «Juniper Research», при сохранении текущего уровня кибератак в ближайшие годы общие убытки мировой экономики от их осуществления к 2019 г. составят 2,1 трлн долл.[4] Что касается именно России, то ущерб от имевших место на ее территории кибератак в 2015 г., например, составил сумму, равную половине затрат российского бюджета на здравоохранение (приблизительно 1 трлн 423 млрд руб.!)[5].

Таким образом, большинство изменений, возникших по причине развития информационных технологий, принесли пользу обществу прежде всего в науке, медицине, инженерии, управлении ресурсами (в т. ч. финансовыми). Однако они же предопределили

---

[1] *Шевченко Е. С.* Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. М.: изд. Группа «Юрист», 2015. № 3. С. 29–30.

[2] *Сачков И.* Технологии позволяют бороться с киберпреступностью – этот бизнес становится неэффективным // Sk.ru, URL: http://sk.ru/news/b/press/archive/2017/12/20/ilya-sachkov-tehnologii-pozvolyayut-borotsya-s-kiberprestupnostyu-_1320_-etot-biznes-stanovitsya-neeffektivnym.aspx (дата обращения: 18.04.2018).

[3] Как современные Шерлоки Холмсы находят интернет-мошенников // Правовая газета «Статус». 2012. № 8. С. 7.

[4] Общемировые убытки от киберпреступности составят $ 2,1 трлн до 2019 года // Режим доступа: URL: http://www.securitylab.ru/news/472924.php (дата обращения: 18.04.2018).

[5] *Трунцевский Ю. В.* Состояние и тенденции преступности в Российской Федерации и прогнозы ее развития // Российская юстиция. 2016. № 8. С. 29–31.

появление новых возможностей для причинения вреда интересам общества и государства, поскольку с появлением технологических новаций возникли основывающиеся на них новые разновидности преступлений, такие, например, как хакерский взлом, внедрение шпионских программ и др. Если бы не технологический прорыв в области информационно-коммуникационных технологий, то, наверное, их бы вообще не существовало в природе.

Главными характеристиками, определяющими то или иное противоправное деяние как киберпреступление, правильнее всего считать его совершение с помощью компьютерных и сетевых технологий. Специалисты в своих трудах справедливо отмечают, что в современных условиях практически все разновидности преступлений могут быть совершены при помощи персонального компьютера, исключая, пожалуй, некоторые преступления против жизни и здоровья граждан[1]. При совершении киберпреступлений нередко осуществляются прямые атаки на компьютеры или другие устройства с целью вывода их из строя. Иногда атакованные компьютеры используются для распространения вредоносных программ, незаконной информации, разного рода изображений (например детской порнографии) и других материалов. В новейшей юридической литературе выделяются следующие виды киберпреступлений: корыстные киберпреступления (фишинг, кибервымогательство, финансовое мошенничество и др.); хищение персональных данных; кибершпионаж; кибербуллинг; нарушение авторских прав и некоторые другие.

Рассматривая их, нужно учитывать, что в современных условиях в легальный экономический оборот активно поступают «нетрадиционные» виды имущества (в т. ч. интернет-сайты, электронные деньги, технологии мобильной связи, интернет-имущество и т. п.)[2]. Поскольку они обладают способностью приносить высокие доходы, на них соответствующим образом реагирует криминальная среда. В результате появляются все новые виды преступных посягательств, предполагающие использование современных информационных технологий на условиях внезапности и анонимности[3]. Практически все названные противоправные деяния значительно опаснее иных преступлений, совершаемых вне киберпространства,

---

[1] См. например: *Степанов-Егиянц В.Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. 190 с.

[2] *Некрасов В.Н.* Актуальные вопросы уголовно-правовой охраны информационной деятельности в России // Актуальные проблемы российского права. 2017. № 7. С. 108–114.

[3] *Рассолов И.М.* Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 44–46.

поскольку обладают способностью причинять ущерб всем охраняемым законом интересам, диапазон которых варьируется от интересов безопасности государства до частных неимущественных интересов отдельных граждан.

Внедрение новых форм банковского обслуживания, например, повлекло за собой разноплановые криминальные угрозы, реализуемые через высокотехнологичные хакерские атаки. Все чаще преступники используют методы социальной инженерии. Посредством их применения владелец счета либо сам переводит свои деньги преступникам, либо добровольно передает им всю конфиденциальную информацию, необходимую для получения доступа к своему счету (в т. ч. персональные данные, сведения о платежных картах, контрольную информацию, пароли). В результате становятся возможными хищения электронных денежных средств с банковских счетов посредством вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. С каждым годом таких хищений совершается все больше и больше. Они уже стали для многих государств серьезной проблемой. В Российской Федерации естественной реакцией на их рост стало усиление уголовной ответственности[1]. Возьмем на себя смелость утверждать, что борьба с киберпреступностью является проблемой международного масштаба, поскольку меры по предотвращению, выявлению, раскрытию и расследованию преступлений, совершаемых с использованием современных информационных технологий, не могут быть результативными лишь на национальном уровне в силу транснационального и трансграничного характера самой сети Интернет. Более того, непрекращающееся увеличение численности ее пользователей закономерно порождает их зависимость от информационного сообщества и уязвимость от разного рода киберпосягательств. Одновременно возрастает вероятность стать очередной жертвой киберпреступности. Именно поэтому одним из принципов Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. провозглашено обеспечение государственной защиты интересов российских граждан в информационной сфере[2]. Особую и ярко выраженную актуальность решение этой задачи приобретает в деле имплементации в научные ресурсы отечественной криминалистики современных информационных технологий.

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23 апреля 2018 г. №111-ФЗ // Рос. газ. 2018. № 7551 (88). 25 апр. .

[2] Стратегия развития информационного общества в Российской Федерации на 2017– 2030 годы. Утв. Указом Президента РФ от 9 мая 2017 г., № 203 // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=216363&rnd=56A7063FB39FE90B711ADF6487C92D5D&dst=100 (дата обращения: 18.04.2018).

Общие и частные векторы совершенствования криминалистических методик расследования на основе внедрения современных цифровых технологий и технических средств

Н. Г. Шурухнов,
главный научный сотрудник
ФКУ НИИ ФСИН России,
профессор кафедры,
доктор юридических наук, профессор

В тезисах представлены отдельные виды криминалистических методических рекомендаций расследования преступлений и предложения по их совершенствованию.

Расследование; методические криминалистические рекомендации; общие положения методики; концепция; общая методика; частная методика; цифровые технологии; информация; информационные технологии; технические средства; автоматизированное (компьютерное) рабочее место (А(К)РМ); мобильное автоматизированное (компьютерное) рабочее место (МА(К)РМ) дознавателя, следователя; видео-регистрация; транскрайбер.

1. Совершенствование, интенсификация, повышение эффективности процесса расследования преступлений осуществляется через внедрение оптимальных методических криминалистических рекомендаций. Идеально, когда их разработка ориентирована на конкретный вид методики, взаимосвязь средств и методов всех разделов криминалистики, с приспособлением цифровых технологий, достижений технических наук к процессу расследования противоправных деяний.

Речь идет о технических средствах, цифровых технологиях, банках данных профильных аналитических систем, комбинированных информационных технологиях обнаружения, фиксации, изъятия и исследования различных следов и вещественных доказательств, анализа большого объема сведений для определения направления расследования, установления обстоятельств совершения преступления, выбора приемов и методов нейтрализации конфликтов участников уголовного судопроизводства, минимизации противодействия дознавателю, следователю.

2. Арсенал научно обоснованных, практически значимых криминалистических рекомендаций должен включать методики рас-

следования отдельных родов, групп, видов преступлений. Такой классификационный подход одновременно обеспечивает их теоретическую и практическую значимость, роль предыдущей методики в построении последующей, исключая повторение, сосредоточивая внимание на инновациях[1]. В системе криминалистических методических рекомендаций ведущее место должно отводиться концепции и частной методике.

3. Концепция расследования определенного рода преступлений представляет собой криминалистические методические рекомендации высокого абстрактного уровня, имеющие несколько взаимосвязанных, взаимообусловленных целей. Ее базой являются теоретико-правовые, научно-методические положения, детерминанты отдельных отраслей права, технико-технологические, организационные и управленческие составляющие, эмпирические данные, полученные в процессе обобщения практики расследования конкретного рода преступлений.

Разработка концепции расследования преступлений предназначена дать родовую криминалистическую классификацию противоправных деяний, отправные положения для построения общих, частных методик и методических рекомендаций, базирующихся на преступлениях, составляющих ее предмет. В задачу концепции входят обоснование системы расследования, представление обобщенной тактики и технологии производства процессуальных действий, специального компьютерного моделирования в планировании расследования, взаимодействия, использования информационных технологий, информационно-телекоммуникационных систем, технических средств, специальных знаний.

4. Частная криминалистическая методика[2] по своему содержанию должна быть конкретной, целенаправленной и представлять полнообъемную систему расследования[3]: раскрывать содержание

---

[1] При формировании собственной позиции мы ориентировались на исследования: О.Я. Баева, Р.С. Белкина, А.Н. Васильева, И.А. Возгрина, А.Ф. Волынского, В.К. Гавло, Ю.П. Гармаева, В.А. Жбанкова, В.Д. Зеленского, Е.П. Ищенко, В.Е. Корноухова, В.П. Лаврова, И.М. Лузгина, Н.Е. Мерецкого, Г.М. Мудьюгина, В.А. Образцова, А.А. Протасевича, Н.А. Селиванова, Д.А. Турчина, А.Г. Филиппова, А.А. Хмырова, В.И. Шиканова, Н.П. Яблокова.

[2] Р.С. Белкин определял ее как «типизированную систему методических (научно-практических) рекомендаций по организации и осуществлению расследования и предотвращения отдельного вида преступлений». См.: *Белкин Р.С.* Курс криминалистики. М.: Юристъ, 1997. Т. 3. С. 301.

[3] Такой подход вытекает из этимологии слова «методика» – совокупность методов, приемов целесообразного проведения расследования, которое не мыслится при отсутствии системы (этапности расследования).

предварительного[1], первоначального, последующего, заключительного этапов расследования. В ней должны быть представлены данные о следах совершения преступлений с использованием информационно-телекоммуникационных технологий, а производство следственных действий включать технологию работы с компьютерными следами. Отдельное место должны занимать цифровые технологии анализа больших объемов сведений, используемые для формирования следственных ситуаций, определения направлений по их оптимальному разрешению, а также в процессе планирования проведения отдельных следственных действий и всего расследования в целом, поддержки принятия различных видов решений.

5. Совершенствование тактики и технологии производства процессуальных действий должно идти векторами использования: а) автоматизированного (компьютерного) рабочего места (А(К)РМ); б) мобильного автоматизированного (компьютерного) рабочего места (МА(К)РМ) дознавателя, следователя[2].

Использование программных цифровых продуктов должно осуществляться на основе формирования кибернетической модели процесса расследования, способной в несколько раз повысить его технологичность и обеспеченность информацией.

Специальное программное обеспечение МА(К)РМ, используемое при расследовании преступлений, должно включать:

– средства доступа к информационным ресурсам, содержащим различные сведения;

– средства доступа к нормативно-правовым базам;

– средства доступа к ресурсам федерального уровня (МВД РФ, СК РФ) – банку процессуальных документов;

---

[1] Более подробно см.: *Шурухнов Н.Г.* Влияние уголовно-процессуального законодательства на структуру расследования преступлений // Уголовное судопроизводство: проблемы теории, нормотворчества и правоприменения: сб. науч. тр. (посв. 5-летию введения в действие Уголовно-процессуального кодекса Российской Федерации). Рязань, 2007. Вып. 2. С. 147–156.

[2] См.: *Шурухнов Н.Г., Гаврилин Ю.В.* Некоторые направления использования автоматизированных рабочих мест при проведении следственных действий // Персональный компьютер на службе криминальной милиции и следствия. Возможности и перспективы: сборник материалов научн.-практ. семинара. М.: ВНИИ МВД России, 1997; *Шурухнов Н.Г.* Мобильное автоматизированное рабочее место следователя (МАРМС) как базовое средство повышения эффективности тактики производства процессуальных действий // Актуальные проблемы криминалистической тактики: материалы Международной научно-практ. конф. (г. Москва, 28 марта 2014 г.). М.: изд-во «Юрлитинформ», 2014. С. 296–305; *Шурухнов Н.Г.* Правовые, материально-технические и организационно-методические основы информационного обеспечения производства процессуальных действий // Актуальные проблемы борьбы с преступностью: материалы межвуз. научно-практ. конф. (Тула, 25 марта 2014 г.). М.: РПА Минюста России, 2014. С. 218–224.

– справочные, экспертно-консультационные системы, например, содержащие алгоритмы действий (следственных, процессуальных, розыскных) в условиях наиболее распространенных следственных ситуаций, комплексы тактических приемов проведения различных процессуальных действий, ссылки на необходимые акты и инструкции;

– программу оформления запросов, поручений, актов, сообщений.

Как представляется, все это должно быть продуктом разработки самостоятельного подраздела криминалистики, посвященного использованию цифровых технологий в расследовании преступлений, о котором говорил доктор юридических наук, профессор кафедры управления органами расследования Академии управления МВД России Ю. В. Гаврилин.

6. Интенсификация производства процессуальных действий будет эффективной в том случае, если в программе МА(К)РМ дознавателя, следователя содержатся:

1) бланки постановлений;

2) образцы писем и запросов (ст. 21, ст. 144 УПК РФ);

3) бланки ходатайств (постановлений) о проведении принудительных следственных действий (ст. 165 УПК РФ);

4) наборы протоколов различных следственных действий;

5) образцы описания различных следов, объектов, предметов;

6) рекомендации по изъятию, упаковке и хранению конкретных образцов;

7) виды научно-технических средств и рекомендации по их применению; 8) наименования специфических объектов;

9) названия и адреса государственных, негосударственных экспертных учреждений, лиц, которые могут проводить экспертизы, выступать в качестве специалистов;

10) вопросы экспертам по различным видам судебных экспертиз;

11) перечень вопросов, наиболее часто задаваемых при допросах различных участников уголовного судопроизводства;

12) рекомендации, советы по выбору тактических приемов проведения отдельных следственных действий;

13) перечень действий и приемов, обязательных при осмотре места происшествия, и порядок их реализации.

7. Оптимальность производства следственных действий в определенной степени зависит от уровня использования новейших технических средств фиксации их хода и полученных результатов. В уголовном судопроизводстве часто используются разнообразные

технические средства, позволяющие осуществить видео – и аудиозапись. Но при этом не применяются автоматизация расшифровки фонограмм, их преобразование в текстовую информацию, перенос на материальный носитель. Для решения этой практической задачи следует использовать цифровой транскрайбер. Его программа обеспечивает оптимальное сочетание свойств современного текстового редактора и функций цифрового магнитофона для быстрого набора текста, обеспечения качества прослушивания звука.

Готовясь к производству следственного действия с использованием транскрайбера, нужно подыскать помещение с максимальной звуковой изоляцией, исключающей посторонние звуки, установить микрофон, снимающий звук, либо диктофон и разместить на одинаковом расстоянии от них активных участников следственного действия.

В заключение производства следственного действия необходимо осуществить упаковку записанной фонограммы, снабдив ее соответствующими надписями и удостоверяющими подписями. Дознаватель, следователь может упаковать весь диктофон либо перенести фонограмму, в присутствии всех участников следственного действия, на компьютер, с которого, после прослушивания, она переносится на диск с калибровкой «R» (с закрытием дальнейшей записи информации). Диск также упаковывается по правилам, установленным уголовно-процессуальным законодательством[1].

8. Транскрайбер может использоваться и в составлении протокола следственного действия. При этом дознаватель, следователь предварительно «наговаривает» на цифровую звукозаписывающую аппаратуру информацию, составляющую содержание протокола, для последующего преобразования в текстовую.

---

[1] См.: *Шурухнов Н.Г.* Процедура и содержание процессуальных информационно-технологических средств сбора доказательств, используемых в российской практике расследования преступлений, совершаемых с использованием современных электронных технологий // Вопросы правоведения. 2013. № 5 (21). С. 294–315.

Цифровая криминалистика как фактор защиты цифровой экономики

А. Н. Яковлев,
доцент,
кандидат юридических наук
(Следственный комитет Российской Федерации)

В статье проанализированы наиболее уязвимые компоненты цифровой экономики – ее технические и технологические компоненты, технологии блокчейн, криптовалюты. Дано определение цифровой криминалистики. Сделан вывод о необходимости изучения особенностей цифровой экономики в аспекте проблем раскрытия и расследования преступлений.

Цифровая экономика, преступление, раскрытие, криминалистика, экспертиза, интернет, криптовалюта.

Большое и пристальное внимание научного сообщества сегодня уделено особенностям цифровой экономики в аспекте проблем раскрытия и расследования преступлений. Это не дань моде, а острейшая потребность дня, это тот круг проблем, который практически не фигурирует в дискуссиях. Это аспект защиты цифровой экономики и масштабное использование в этих целях возможностей цифровой криминалистики.

Непосвященному в специфику проблем цифровой экономики кажется, что проблем с ее защитой нет. При этом в качестве аргументов «беспроблемности» будут фигурировать ссылки на детализированное в аспекте борьбы с киберпреступностью российское и международное уголовное законодательство, адаптированный к борьбе с киберпреступностью уголовно-процессуальный кодекс, адаптированную к цифровизации общества криминалистику и судебную экспертизу, получившие новые важные компоненты в форме цифровой криминалистики и компьютерно-технической экспертизы.

К сожалению, оперируя лишь перечисленными аргументами, мы ошибаемся, потому что плохо различаем два существенно разных понятия – цифровизацию общества и цифровую экономику.

Цифровизация общества является лишь очередным аспектом информатизации, качественно иным, принципиально меньшего масштаба, чем цифровая экономика. Цифровизация общества позволяет достаточно легко адаптировать действующее законодательство, криминалистику и судебную экспертизу под обновленные задачи

и потребности общества, потому что технологическая платформа внедряемых решений создавалась постепенно на предшествующих этапах информатизации и сопровождалась постепенным же изменением законодательства.

А вот цифровая экономика определенно делает нереализуемым «легкий адапционный флирт», предполагая и требуя глобальных перемен в уголовном и уголовно-процессуальном законодательстве, а также такого кардинального изменения криминалистики и судебной экспертизы, которое по масштабам можно назвать их перестройкой.

Такое предположение обусловлено не субъективной оценкой ситуации, а объективной реальностью – цифровая экономика уже в момент своего становления максимально не защищена, и прежние адаптационные механизмы законодательства, криминалистики и судебной экспертизы в условиях цифровой экономики все хуже и хуже работают. Сегодня на всех уровнях компетентности следует развернуть дискуссии о различных аспектах беззащитности цифровой экономики перед большим спектром угроз, озвучить её болевые точки и приступить к разработке предложений по их нейтрализации.

Нам представляется необходимым выделить и минимально рассмотреть три самых уязвимых компонента цифровой экономики: ее технические и технологические компоненты, технологии блокчейн, криптовалюты.

Рассмотрим проблемы, связанные с ***техническими и технологическими компонентами цифровой экономики***.

По данным прошлого года, общий ущерб от киберпреступлений в корпоративном и частном секторах составил 2,9 млрд руб. Безусловно, это много. Но ущерб от коррупции в это же время составил 78 млрд руб. Почти в 30 раз больше. Такое соотношение подтверждает непубличные выводы специалистов по информационной безопасности о том, что оценка тяжести экономических последствий киберпреступности завышена, в том числе в целях выделения этой отрасли повышенных бюджетов. Да, в информационном обществе, особенно в условиях его дальнейшей цифровизации важно, иногда критически важно, уметь противостоять киберпреступлениям. Но все-таки сопоставление абсолютных показателей ущерба от разных категорий преступлений свидетельствует о том, что сегодня проблема киберпреступности не является доминирующей и нужно обратить свое внимание на иные, возможно, только нарождающиеся виды высокотехнологичных преступлений.

Официальных данных об ущербе от преступлений в сфере цифровой экономики пока нет, поскольку цифровая экономика только начинает функционировать. Однако уже сейчас можно определить ключевые составляющие такого ущерба. Он будет включать:

1) существенную часть того ущерба, который ранее мы относили к «чистой» киберпреступности. Например, если до эпохи цифровой экономики атака типа DDoS была атакой на отдельный сетевой ресурс, то в эпоху цифровой экономики DDoS-атака становится атакой на «внешний» WEB-компонент сложной информационной системы, относимой уже к системам цифровой экономики, и тип атаки будет отнесен обновленным классификатором не к киберпреступности, а к преступлениям в сфере цифровой экономики;

2) ущерб от преступлений, совершаемых при разработке и реализации проектов информационных систем (уже сейчас это огромные суммы);

3) ущерб от аналога экономических преступлений, но совершаемых в цифровой среде в отношении субъекта цифровой экономики (сюда начинает «уходить» и в будущем «уйдет» весь нынешний и будущий ущерб от «обычных» преступлений в сфере экономики).

Таким образом, финансовая составляющая преступного интереса к цифровой экономике уже сейчас очевидна.

Как будут проводиться в изменившихся условиях оперативно-розыскные мероприятия и следственные действия, в целом представляется ясным. Новыми положительными факторами расследования станут государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), технологии BigData, сервисы служб информационной безопасности компаний, современные технологии оперативно-розыскной работы, следственных действий и компьютерной (компьютерно-технической) экспертизы. Однако большой проблемой является то, что при создании, функционировании, развитии перечисленных компонент интересы цифровой экономики не учитывались по объективным и субъективным причинам. В результате, например, система обнаружения, предупреждения и ликвидации последствий компьютерных атак на ИТ-ресурсы, расположенные на территории России, больше ориентирована на решение задач информационной безопасности, нежели на решение задач доказывания.

Аналогичное замечание можно сделать и в отношении технологий BigData. Их правовое обеспечение не ориентировано на расследование преступлений. Например, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) под угрозой больших штрафов запрети-

ла компаниям собирать общедоступные данные пользователей на страницах социальных сетей и сайтов вне зависимости от цели сбора, посчитав эти данные персональными. Такой подход регулятора к оценке общедоступных данных существенно ограничивает возможности служб информационной безопасности в расследовании инцидентов, а правоохранительные органы – в расследовании преступлений.

Распространение требований регулятора к обработке персональных данных на криминалистические инструменты обработки общедоступной информации создает неразрешимые проблемы. Например, сложно оценить объем обрабатываемых данных, если проводится так называемый «глубокий» поиск по всем общедоступным ресурсам сети Интернет. Относительно собственно криминалистических программных инструментов возникает проблема противоречивости требований типа «казнить нельзя помиловать»: в соответствии с целью сбора общедоступных данных такие программы должны работать во внешнем контуре и «глядеть» в Интернет, но в соответствии с политиками безопасности эти же программы должны находиться во внутреннем, защищенном контуре безопасности информационных систем правоохранительных органов.

Сервисы служб информационной безопасности компаний – это отдельный проблемный фактор в защите цифровой экономики. Их многолетнее ориентирование исключительно на защиту информации в ситуации, когда правоохранительные органы только адаптировались к новому для них виду преступности, было вынужденным. Однако впоследствии, когда правоохранительные органы стали нуждаться именно в доказательственной информации, оказалось, что все технологии защиты информации ориентируются на пресечение атак здесь и сейчас, а не на выполнение уникальных требований по фиксации цифровой информации и превращение ее в доказательство. В настоящее время только Банк России выполнил необходимую подготовительную работу, по итогам которой разработал совместно с цифровыми криминалистами стандарт СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении инцидентов информационной безопасности и реагировании на них при осуществлении переводов денежных средств». Это позволяет надеяться на то, что кредитно-финансовые учреждения первыми смогут использовать весь спектр возможностей защиты цифровой экономики – от технических средств до правовых, реализуемых совместно с правоохранительными органами.

Требуют пересмотра привычные методы и средства оперативно-розыскной деятельности, следственных действий и компьютер-

ной (компьютерно-технической) экспертизы. Что хорошо работало совсем недавно, сегодня работает все хуже и хуже. Приведем небольшой пример. Сегодня или завтра в ходе оперативно-розыскных или следственных действий владельцы информации обеспечат доступ сотрудникам правоохранительных органов для поиска ориентирующей или доказательственной информации уже не к RAID-массиву сервера объемом пару десятков терабайт, а к распределенной корпоративной или государственной информационной системе, в которой вся криминалистически значимая информация будет содержаться в сложнейших виртуальных машинах на огромных по объему серверах. Имеются ли сегодня технологии получения такого доступа даже при условии согласия владельца информации? Технологии поиска нужных данных в огромных массивах? Технологии выгрузки как данных, так и их метаданных, новых неизвестных сегодня видов и форматов для последующего использования в судопроизводстве? Положительные ответы на эти вопросы сегодня отсутствуют.

Рассмотрим проблемы, связанные с ***технологией блокчейн***.

Будет справедливым сказать, что первым разработчиком этой технологии был не полумифический Сатоши Накамото, а группа математиков государственного во времена СССР фундаментального института академии наук, которые в прошлом веке придумали такую технологию и назвали «накоплением контрольных сумм».

Уже тогда была доказана узкая применимость технологии, поскольку расчеты показывали, что при применении в государственном масштабе реализация технологии за месяцы заполнит «контрольными суммами» весь объем памяти всех больших ЭВМ страны. По большому счету, и сейчас мало что изменилось: при непродуманном внедрении кумулятивные последствия технологии блокчейн не будут сильно отличаться от эффекта «червя Морриса», который когда-то в США перегрузил мощности сетевых компьютеров так, что это стало предметом судебного разбирательства. В нынешнем виде технология блокчейн уместна для применения лишь в масштабах организации, возможно, ведомства, если у последнего хватит объемов дисковой памяти.

Следующий критический компонент цифровой экономики – ***криптовалюты***.

Отдельно стоит сказать о майнинге криптовалют. В информации от известных компаний, исследующих тенденции глобальных угроз безопасности, говорится о двух крайне тревожных сигналах:

– никто не знает алгоритмов майнинга, кроме их создателей; чем фактически занимаются миллионы компьютеров по всему миру, достоверно неизвестно;

– компьютеры в процессе майнинга нагружены так интенсивно, что в прямом смысле слова вызывают пожары; однако специалистам сегодня не известна сопоставимая по эффекту энергозатрат какая-либо расчетная деятельность, которая приводила бы к схожей нагрузке на вычислительное средство.

В качестве правдоподобной выдвигается версия, в которой некоторая страна придумала концепцию не только добровольного предоставления ей чужих вычислительных мощностей, но и оплаты такой «аренды» не из собственных средств, а вычисляемыми попутно виртуальными «фантиками». Поэтому сегодня в равной степени можно предполагать, что участвующие в «майнинге» криптовалют компьютеры рассчитывают параметры массированного ядерного удара или глобального изменения климата.

О самих криптовалютах.

Министерство финансов Российской Федерации опубликовало проект закона «О цифровых финансовых активах», посвященного регулированию операций с криптовалютой в России. Сейчас это серая зона в российском законодательстве. Сделки с криптовалютой не запрещены, но сами по себе подобные операции считаются достаточным основанием для проверки на причастность к отмыванию доходов, полученных преступным путем, или финансированию терроризма.

Закон оговаривает следующие ограничения на покупку и продажу биткоинов. Все сделки по покупке, продаже или обмену одной криптовалюты на другую будут осуществляться только через операторов обмена цифровых финансовых активов, в качестве которых будут выступать российские юридические лица, имеющие лицензии биржи или лицензии торговой системы. Оператор обмена цифровых финансовых активов станет владельцем кошелька, а пользователь будет только иметь один из ключей, с помощью которого можно будет подписывать распоряжения на операции с содержимым кошелька. Операции со средствами в кошельке, заведенном и используемом не по правилам, вне контроля Банка России, будут считаться незаконными.

В итоге нас ждет официальный и теневой рынок расчетов, в котором будут зафиксированные и контролируемые государством транзакции криптовалют, и иные – к которым относятся все нынешние транзакции. К такому изменению рынка безналичных расчетов нужно готовиться современной правоохранительной системе.

Перечень проблем можно продолжать, однако решение их сегодня может быть найдено, по нашему мнению, только в усиленной и ускоренной разработке положений цифровой криминалисти-

ки, которая надолго становится одним из самых существенных факторов защиты цифровой экономики.

Это связано с тем, что цифровая криминалистика удостоверяет научную надежность положений традиционной криминалистики. Цифровая криминалистика – это лишь обозначение особенностей выявления следующих уголовно-релевантных закономерностей.

1. Закономерностей преступной деятельности, направленной на воспрепятствование нормального функционирования информационных систем, их компонент. Это важно, поскольку в цифровой экономике многое в такой деятельности становится принципиально новым, о чем мы упоминали.

2. Особенностей преступной деятельности, направленной на использование информационных систем, их компонент в качестве инструмента совершения иных преступлений. Спадает пелена с глаз, и мы все громче говорим о том, что с использованием термина «компьютерные преступления» были некоторые перегибы; что наши учителя были мудрее и не называли преступления, для подготовки и совершения которых использовался дисковый аналоговый телефон, «телефонными». В общей части многих уголовных кодексов зарубежных стран сегодня содержится базовое положение о том, что все изложенное в кодексе в равной степени относится к данным в электронной (цифровой) форме. Кодексы не перегружены статьями с примечаниями. Зарубежные криминалисты воспринимают цифровую составляющую жизни не как революцию в криминалистике, а как существенные, но лишь особенности традиционной криминалистики. Цифровая экономика неизбежно приведет нас к пересмотру нынешнего уголовного кодекса.

3. Особенностей создания, изменения, передачи, удаления информации на электронных носителях, в информационно-телекоммуникационных сетях, виртуальном пространстве, связанных с подготовкой, совершением, сокрытием преступлений. Цифровая криминалистика позволяет нацелить все госструктуры, службы информационной безопасности на компетентный подход в поиске и фиксации цифровых доказательств.

4. Особенностей исследования цифровой информации, сохраненной в отдельных информационных объектах, а также в информационной среде электронного носителя информации.

Подводя итог сказанному, следует сказать, что в отношении цифровой криминалистики и защиты цифровой экономики актуален известный лозунг «Вчера было рано, завтра будет поздно», поэтому важен факт своевременного начала дискуссии по этим проблемам.