МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М.В. ЛОМОНОСОВА

ЭЛЕКТРОННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ В КРИМИНАЛИСТИКЕ

(сборник докладов круглого стола 13.05.2016 г.)

г. Москва
2016

УДК 344.9
ББК 68.520

Печатается по решению кафедры криминалистики Московского государственного университета имени М.В. Ломоносова

Электронные носители информации в криминалистике: материалы круглого стола, МГУ, Москва, 13.05.2016 / под ред. проф. Кучин О.С. – М.: МГУ, 2016. – 74 С.

ISBN 978-5-318-05164-1

Сборник сформирован по материалам выступлений на круглом столе, проходившем на кафедре криминалистике Юридического факультета Московского государственного университета имени М.В. Ломоносова 13 мая 2016 г. В нём представлены научные статьи учёных в области криминалистики.

Предназначен для научных работников, преподавателей, аспирантов и студентов юридических факультетов.

ББК 68.520

ISBN 978-5-318-05164-1

Издательство МГУ, 2016.

С О Д Е Р Ж А Н И Е:

Алиева Г.А.

Роль электронных носителей информации и информационных технологий в расследовании взяточничества и коммерческого подкупа в ЖКХ

Группа преступлений в сфере ЖКХ, заявленная в теме настоящей статьи, характеризуется тем, что в настоящее время способ их совершения становится все более изощренным: привлекаются несколько посредников; незаконное вознаграждение выступает в качестве «откатов» от полученных бюджетных средств на капитальный ремонт, благоустройство и пр.; выводятся в оффшорные зоны и др. Средствами, благодаря которым реализуются такие схемы, выступают в том числе современные информационные технологии.

В связи с этим возникает объективная потребность следователя в использовании знаний сведущих лиц в области информационных технологий (включая потребность в знаниях по фиксации, изъятию, копировании, транспортировке и хранении электронных носителей информации). Следственная практика показывает, что зачастую следователи прибегают к помощи специалистов экспертно-криминалистических подразделений МВД России, Института ЦСТ ФСБ России. Совместно с ними к участию привлекаются специалисты отделов документальных проверок и ревизий управлений экономической безопасности и противодействия коррупции управлений внутренних дел МВД России по субъектам РФ. Проведение ими исследований предметов и документов в данном случае имеет важное значение, так как по современным преступлениям в сфере ЖКХ осуществляются сложные схемы приема - передачи предмета взятки или незаконного вознаграждения при коммерческом подкупе, при этом оформляются большое количество электронных

документов: бухгалтерских, финансово-расчетных и пр., осуществляется значительное количество банковских операций и тд., что маскирует преступную деятельность под правомерное осуществление должностным лицом или лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий.

Особенно необходимо привлекать специалистов к производству обысков в служебном кабинете, квартире подозреваемого, подсобных помещениях, гаражах, в квартирах его родных и близких лиц, их дачах и др., когда перед следователем стоит задача своевременного обнаружения, фиксации и изъятия объектов на электронных носителях, наряду с документами, имеющими признаки подделки, подчисток, дописок или травления; незаконно полученных документов; документов с содержанием недостоверных сведений; недействующих документов и т.д. Указанные признаки могут свидетельствовать о совершении должностным лицом или лицом, выполняющим управленческие функции в коммерческой или иной организации в сфере ЖКХ, определенных действий по подготовке, совершению и сокрытию преступления. Наряду с применением научно-технических средств, специалист сообщает следователю ориентирующую информацию об особенностях искомых объектов, которые возможно обнаружить в ходе производства обыска. Обычно, такими сведениями располагают специалисты, принимавшие участие в осмотре места происшествия по уголовному делу о взяточничестве или коммерческом подкупе в ЖКХ, так как у последних имелась возможность проанализировать механизм его совершения и условия следообразования.

При производстве выемки и обысков по уголовным делам рассматриваемой группы преступлений все чаще обнаруживаются объекты, квалифицированное описание и изъятие которых без специалистов не представляется возможным. К таковым относятся как носители электронной информации[1] (стационарные компьютеры, планшеты, гаджеты, мобильные телефоны, внешние жесткие диски,

[1] См. : п. 3.1 ст. 183 УПК РФ.

видеорегистраторы и др.), так и неправомерно списанная уборочная, коммунальная, дорожная техника. Наряду с этим, проведенный автором опрос свидетельствует о том, что при расследовании взяточничества или коммерческого подкупа в ЖКХ 31 % респондентов прибегали к помощи специалистов при осмотре документации, изъятой на электронных носителях, 6 % - затрудняются ответить на данный вопрос, 53 % опрошенных – не привлекали к участию лиц, обладающих специальными знаниями.

В свою очередь, привлечение специалистов помогает следователю определить особенности каждого из указанных объектов, функциональную часть, техническую документацию и т.д., способствует переносу хранящейся на электронных носителях информации на лазерные диски. Кроме того, при производстве данного следственного действия помощь специалиста будет выражаться в отборе объектов, которые будут использованы в качестве образцов для сравнительного исследования при назначении судебных экспертиз (фоноскопических, почерковедческих, технико-криминалистических и др.).

Следует отметить, что подготовка к передаче - получению предмета взятки или незаконного вознаграждения в ЖКХ может осуществляться с использованием информационных технологий (переписка в Интернет-сайтах, использование программ для мгновенного обмена сообщениями и др.). Кроме того, передача денежных средств может осуществляться посредством электронных платежных систем («Яндекс. Деньги», «Деньги@Mail.ru», «Webmoney», «Rapida», «PayPal», «Qiwi» и др.). При указанных обстоятельствах использование специальных знаний при расследовании данной группы преступлений в сфере ЖКХ возрастает.

Помощь специалиста также возможна и после получения заключения эксперта. Учитывая, что заключение эксперта является доказательством по уголовному делу, полученным с использованием специальных знаний, оно представляет определенную сложность во всесторонней оценке для следователя. В связи с этим требуется помощь лица, обладающего соответствующими познаниями. Вместе с тем, результаты проведенного опроса показывают, что

лишь 2 % респондентов привлекали специалистов для оценки заключения эксперта по уголовным делам о взяточничестве или коммерческом подкупе в ЖКХ.

Таким образом, подводя итог изложенному, можно сделать вывод о том, что без использования знаний сведущих лиц при расследовании взяточничества и коммерческого подкупа в сфере ЖКХ, следователю сложно разобраться в многоуровневых способах приема - передачи предмета взятки или незаконного вознаграждения при коммерческом подкупе, где преступники все чаще используют современные информационные технологии с целью подготовки и сокрытия следов преступления.

Аминев Ф.Г.
к. ю.н. доцент

Об использовании компьютерных технологий в обучении криминалистике и судебной экспертизе

В условиях продолжающей оставаться сложной криминогенной обстановки в Российской Федерации[2], совершенствования преступниками способов и форм своих противоправных действий[3], всё большее внимание уделяется профессиональной подготовке сотрудников следственных, оперативных и экспертно-криминалистических подразделений. Одной из ведущих научно-учебных дисциплин, обеспечивающих профессиональную подготовку названных служб, является криминалистика[4]. По нашему мнению, в процессе

[2] В течение 2015 года в РФ зарегистрировано 2352,1 тыс. преступлений, или на 8,6% больше, чем за аналогичный период прошлого года. Не раскрыто 1026,2 тыс. преступлений, что на 8,2% больше аналогичного показателя за январь-декабрь 2014 года. Ущерб от преступлений составил 436,49 млрд руб., что на 24,9% большего аналогичного показателя прошлого года. // Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2015 года // Состояние преступности (архивные данные): Статистика и аналитика [Электронный ресурс]: Официальный сайт Министерства внутренних дел Российской Федерации, 2016. Режим доступа: https: // https://mvd.ru/folder/101762/item/7087734/, свободный (дата обращения: 15.04.2016.).

[3] Комаров И.М., Пономаренко Н.Ю. Тактические и оперативно-тактические операции как средство собирания доказательств преступления // Современная криминалистика: проблемы, тенденции, перспективы: материалы Международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Николая Павловича Яблокова. Москва, 22 декабря 2015 г. М.: МАКС Пресс, 2015. С. 267.

[4] Кучин О.С. О необходимости постоянного закрепления в УПК РФ разработок криминалистической науки// // Современная криминалистика: проблемы, тенденции, перспективы: материалы Международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Николая Павловича Яблокова. Москва, 22 декабря 2015 г. М.: МАКС Пресс, 2015. С. 142.

профессионального обучения вышеперечисленных категорий служащих, кроме изучения правовых, организационных, методических основ деятельности, включающих современные достижения криминалистики и судебной экспертизы в области собирания, исследования и использования доказательств, должны быть использованы и новые инновационные обучающие технологии: возможности сетевых компьютерных систем, фотограмметрических программ, видео-конференц связи и т.д.

Первостепенное внимание должно быть уделено вопросам получения и совершенствования умений и навыков собирания криминалистически значимой информации при проведении различных процессуальных действий. От проводимых в учебных аудиториях занятий с применением аудио-, видеотехники, цифровых проекторов и других средств обучения, но вне смоделированной конкретной обстановки (в магазине, на предприятии, сквере, уличном перекрестке т.д.), вряд ли можно ожидать прочного усвоения учебного материала. И даже в вузах, ведущих подготовку экспертных кадров, выполняемые студентами учебные экспертизы представляют собой решение облегченных экспертных задач, не могущих отражать в полной мере динамику изменений объектов на практике[5].

Поэтому практические занятия по профилирующим дисциплинам (криминалистика, предварительное следствие, теория оперативно-розыскной деятельности и др.) должны проводиться в специально оборудованных высокотехнологичных учебных полигонах с использованием компьютерной техники, стационарных средств видеозаписи и др. Полигон (от греч. *polygonos* – многоугольный) – обширный участок суши или моря, оборудованный для учебных стрельб, для производства испытаний различных видов вооружения, боевой и некоторых иных видов техники[6]. Криминалистические полигоны

[5] См.: Зинин А.М. Некоторые проблемы подготовки экспертов // Актуальные проблемы судебно-экспертной деятельности в уголовном, гражданском, арбитражном процессе и делам об административных правонарушениях: материалы Международной научно-практической конференции. г.Уфа, 1 октября 2015 года. Уфа: РИЦ БашГУ, 2015. С. 123.

[6] Краткий словарь иностранных слов / Сост. С.М. Локшина. М.: Рус. яз., 1979. С. 213.

позволяют проводить групповые занятия с элементами деловой (ситуационно-ролевой) игры.

Высокая эффективность практического занятия достигается интеграцией смоделированной на криминалистических полигонах обстановки и программно-аппаратного комплекса. Внедрение в этот процесс компьютерной техники обусловлено следующими факторами:

– скорость и безошибочность обработки любого вида информации;

– возрастание возможностей предъявления учебной информации;

– реальность моделирования с помощью компьютера различных процессов;

– компьютерная техника позволяет активизировать содержательную, операционную и мотивационную стороны процесса обучения;

– возможность оптимально дифференцировать учебную деятельность обучаемых в зависимости от уровня подготовки, познавательных интересов и т.д.;

– инновационное оборудование позволяет формировать у обучаемых рефлексию своей деятельности;

– компьютерная техника создает условия для овладения обучаемыми способами организации собственной учебной деятельности;

– высокотехнологичное оборудование играет роль средства учебной коммуникации и т.д.

Для функционирования вышеописанного комплекса криминалистических полигонов они оснащены высокотехнологичными компьютерными средствами и оборудованием: комплектами стационарных цифровых видеокамер с установкой по две камеры в каждом помещении полигонов; программно-аппаратным комплексом с сетевым программным обеспечением на неограниченное количество рабочих мест; аудио-усилителем с селектором; звуковыми колонками; микрофонами; интерактивными досками с мультимедийными проекторами; комплектами операторских рабочих мест клиента видеосервера и т.д.

Анализ проводимых преподавателями Института права Башкирского государственного университета и Уфимского юридического института

практических занятий на высокотехнологичных криминалистических полигонах позволили прийти к ряду выводов:

1. Должна быть четкая дифференциация функций всех лиц, задействованных в организации и проведении данных занятий. Так, проведение занятий в комплексе криминалистических полигонов, организация видеоконференций осуществляется профессорско-преподавательским составом кафедр криминалистики и уголовного процесса. Обслуживание систем видео- и аудио- контроля, компьютеризированных рабочих мест следователя, обеспечение взаимосвязей между отдельными элементами системы, обеспечение видеоконференц-связи осуществляется отделом технических средств обучения (или информационным центром).

Организацию хранения и использования цифровой видеозаписи практических занятий, обеспечение и разграничение доступа к ним осуществляется кафедрой криминалистики совместно с отделом технических средств обучения (информационным центром).

2. Высокотехнологичный мультимедийный обучающий комплекс должен быть реализован на комплексе учебных полигонов с обстановкой, максимально приближенной к реальной. Это способствует формированию у студентов и курсантов навыков:

1) интегрирования разноотраслевых знаний о деятельности по раскрытию и расследованию преступлений;

2) самостоятельного управленческого мышления;

3) нахождения оптимального тактического решения и его грамотного оформления в определенной следственной ситуации;

4) обращения с криминалистически значимой информацией (получения, оформления, анализа, поиска);

5) согласованной работы в локальном специализированном коллективе;

6) активизации творческого криминалистического мышления в сложной ситуации.

3. Роль эффективного средства развития творческих способностей обучаемых выполняет компьютерная техника и ее функционирование в сетевом формате. Поэтому для улучшения качества обучения, повышения практической направленности, качества самостоятельной подготовки курсантов и студентов необходимо провести комплекс мероприятий по созданию в учебных аудиториях, и, по возможности, в общежитиях, точек доступа с последующим их подключением к электронным образовательным ресурсам.

4. Одно из основных назначений компьютерной техники в образовательном учреждении – организация работы обучаемых посредством автоматизированных обучающих систем (АОС), учитывающих перспективные дидактические и психологические концепции, содержание и логику предмета, методику его преподавания. АОС обеспечивают постоянный контакт с каждым обучаемым в режиме диалогового взаимодействия. Помимо этого в комплексе полигонов установлены программно-технические комплексы: мобильный комплекс «Папилон – М (МКДС-40)», «Портрет-Поиск» и др., которые необходимы для ознакомления студентов и курсантов с возможностями этих систем и научат применять их в своей практической деятельности.

5. В практическом занятии на высокотехнологичных мультимедийных полигонах, состоящем из вводной, основной и заключительной частей, следует обратить особое внимание на проведение последней части занятия. В заключительной части занятия преподаватель просматривает совместно с курсантами и слушателями видеозапись работы группы, производит разбор недостатков, допущенных в ходе проведения следственного действия, отмечает положительные моменты, дает рекомендации. Показывает видеофильм о действиях преступника, подготовленный заранее до занятия на месте производства следственного действия, подводит итоги.

После проведения занятия курсантам и студентам предоставляется доступ к видеофрагментам о выполненных ими на занятиях действиях. Во время самостоятельной подготовки с компьютеризированных рабочих мест,

расположенных в аудиториях (общежитии), курсанты и студенты, используя вышеназванные видеофрагменты, должны с учетом указанных недостатков еще раз проанализировать действия, составить протокол следственного действия, а также выполнить другие задания, определенные преподавателем.

Записанные на компьютерные носители видеофрагменты учебных действий можно в дальнейшем использовать для анализа результатов занятий и совершенствования методики их проведения, а также для подготовки учебных фильмов по технике выявления, фиксации, изъятия вещественных доказательств и иных объектов, тактике проведения следственных действий, методике раскрытия и расследования отдельных видов преступлений.

Кроме того, возможно проведение занятий с использованием видеоконференц-связи. При проведении занятия в режиме видеоконференции обсуждение выполняемых действий может производиться с участием более широкой аудитории, в том числе с участием профессорско-преподавательского состава других вузов системы МВД России и с практическими сотрудниками ОВД (включая слушателей заочного обучения – через сеть ЕИТКС МВД России). Также с использованием видеоконференц-связи может проводиться дополнительное консультационное обучение с участием опытных специалистов ОВД и научных учреждений, а также оценка действий обучаемых.

Исходя из того, что технологии представляют собой процессы, при которых происходит качественное изменение обрабатываемого объекта[7], целью использования высокотехнологичных средств и методов в обучении криминалистике и судебной экспертизе является способствование получению сотрудника, обладающего широким спектром знаний, умений и навыков расследования и раскрытия преступлений. Такое понимание использования компьютерных технологий в обучении соответствует принципиальным положениям системного подхода в криминалистике и судебной экспертизе, значение которого подчеркивает проф. Н. П. Яблоков: «Системность выступает

[7] См.: Краткий словарь иностранных слов / Сост. С.М. Локшина. – М.: Рус. яз., 1979. – С. 283.

одним из основополагающих условий должного существования, целостности и дальнейшего развития, в том числе и системы криминалистики как прикладной юридической науки, ее отдельных частей, разделов и теорий»[8]. Результатом такого подхода и должна явиться разработка современных компьютерных технологий обучения криминалистике и судебной экспертизе.

Арипов Т.Э.
к.ю.н., доцент

Соотношение противодействия установлению истины и состязательности сторон

Начиная с 1990-х гг., преступность, становясь всё более организованной и профессиональной, перманентно продолжает расширять масштабы и формы влияния на деятельность органов расследования. Противодействие расследованию, носившее в большинстве своем единичный и разрозненный характер, постепенно трансформировалось в социальное явление.

Только в последнее время противодействию расследованию стало уделяться особое внимание, хотя оно всегда было характерно для преступной деятельности и следственной практики. Раньше противодействие рассматривалось в рамках сокрытия преступления как одного из элементов способа преступления в трудах ученых-криминалистов Р.С.Белкина, А.М.Ларина, В.П.Бахина, И.Е.Быховского, О.Я.Баева, Л.Я.Драпкина. Однако это были в основном упоминания о противодействии как о разновидности конфликтного поведения в деятельности следователя. Лишь В.Н.Карагодин и С.Ю.Журавлев (под научным руководством Р.С.Белкина с 1989 года) в своих трудах подвергли это явление системному

[8] Яблоков Н.П. Системные исследования в криминалистике. Общие вопросы./ Проблемы системных исследований в криминалистике и судебной экспертизе: конференция, 4-5 декабря 2006 г., М.МГУ им М. В. Ломоносова. Сб. тезисов. – М.: МАКС Пресс, 2006. – С. 8.

анализу, положив тем самым начало теперь уже популярной теме противодействия установлению истины [9].

Благодаря успешному противодействию немало преступлений оказывается нераскрытыми, и как следствие: множество нераскрытых преступлений, расследуемых годами; длительная латентность; недостаточная защита прав и интересов потерпевших; формирование недоверия общества к правосудию; усиление коррупционной составляющей в работе органов правосудия, деморализующее влияние противодействия на самих работников правоохранительных органов. Влияние противодействия расследованию на раскрываемость преступлений в качестве решающего фактора провала расследования на сегодня - предмет повышенного интереса для криминалистов, криминологов и актуальная задача для практических работников.

Закон, предоставляя подозреваемым и обвиняемым право на защиту от обвинения всеми возможными средствами в рамках закона, фактически позволяет осуществить это право, в том числе и прибегая к противодействию расследованию: дача ложных показаний, отказ от дачи таковых, немотивируемое (голое) отрицание фактов, умолчание о фактах, неявка по вызову следственных и судебных органов, несообщение запрашиваемых сведений и невыдача требуемых объектов (предметов, документов), неоказание помощи, невыполнение требуемых действий и отказ от участия в следственных действиях, различного рода инсценировки, симуляции психических и иных заболеваний, изменение признаков внешности, иные попытки ввести следствие в заблуждение. Они уголовно не наказуемы и вряд ли противоречат конституционным принципам уголовного судопроизводства, включая состязательность сторон.

С другой стороны, противодействие расследованию не всегда подразумевает защиту от уголовного преследования. Некоторые проявления противодействия влекут не только уклонение виновных от ответственности, но и

[9] Карагодин В.Н. Преодоление противодействия предварительному расследованию. -Свердловск, 1992. *Журавлев С.Ю.* Противодействие деятельности по раскрытию и расследованию преступлений и тактика его преодоления: Автореф. дис... канд. юрид. наук.- Н.Новгород, 1992.

включают незаконные, а иногда откровенно преступные приёмы: подкуп (в этом случае сами лица, осуществляющие предварительное следствие или дознание становятся субъектом противодействия), побег из-под стражи, привлечение СМИ (в т.ч. интернет-ресурсов, включая зарубежных) для создания ажиотажа вокруг расследования в отношении якобы «невиновных», организация и проведение митингов в их поддержку, организация «заказных статей», пикетирования зданий правоохранительных органов под видом «борьбы за охрану демократических прав человека», формирование ложного общественного мнения, требования от властей установить «особый контроль» над расследованием, публикации «компрометирующих материалов» в отношении добросовестного следователя, их толкование во вред расследованию, посягательства на жизнь и здоровье участников процесса (свидетелей, потерпевших), а в некоторых случаях – самого следователя и оперативных работников (угрозы, клевета, провокация, шантаж, похищение близких лиц, физическое насилие, вплоть до убийства) и, наконец, использование коррумпированных должностных лиц правоохранительных органов. К сожалению, следователь подчас перекладывает всю тяжесть поиска подозреваемого, похищенного имущества или изобличения задержанного на потерпевшего, который сам при такой пассивности следователя вынужден заниматься «личным сыском». Полагаться при этом на объективность и полноту установления истины не приходится. А уж тем более у такого «уполномоченного» потерпевшего легко может появиться соблазн преувеличить размер нанесенного имущественного ущерба, ухудшить положение обвиняемого. Либо следователь, идя на поводу «версии потерпевшего», не вникает в возможные мотивы его заявления, представляющего собой оговор невиновного человека.

В некоторых случаях преступникам удается уйти от ответственности, благодаря подделке с использованием современных технических средств документов, удостоверяющих личность, что позволяет преступнику выдавать себя за другого человека и беспрепятственно покидать пределы разыскивающего его государства, принимать безнаказанно участие в террористической деятельности.

В этой связи большинство государств (в т.ч. Узбекистан и Россия), следуя рекомендациям ИКАО (Международной организации гражданской авиации), переходят к биометрической паспортной системе, основанной на идентификации человека по отпечаткам пальцев. Таким образом, необходимость в дальнейшем совершенствовании технико-криминалистических разработок в области дактилоскопии продолжает сохранять свою актуальность.

В связи с увеличением миграционных процессов на пространстве СНГ следователи нередко сталкиваются с противодействием, когда после признательных показаний лицо, по национальности не относящееся к титульной нации, начинает заявлять, что «не понимает языка» судопроизводства и требует предоставить переводчика или сменить переводчика, якобы «не справляющегося» со своими обязанностями.

В таких условиях, когда преступная деятельность всё больше сопровождалась прогрессированием противодействия расследованию, в независимых государствах на пространстве СНГ были приняты уголовно-процессуальные кодексы, основанные на принципе состязательности сторон. Данное нововведение было воспринято многими учеными неоднозначно. Их значительная часть уверена, что введение УПК РФ негативно повлияло на раскрываемость преступлений, а это повлекло нарушение конституционных прав граждан на их защиту от преступных посягательств.

По мнению некоторых из них, возведенный УПК РФ во главу угла принцип состязательности стал весьма мощным рычагом противодействия [10]. В УПК РФ принцип состязательности поставлен выше цели достижения истины, традиционно рассматриваемой в качестве цели доказывания. Если в УПК РУ принцип установления истины нашел свое законодательное закрепление, то в системе принципов российского уголовного процесса положение об объективной истине не нашло своего отражения. Ведущее положение стал занимать принцип

[10] Гаврилов Б.Я. Современная уголовная политика России: цифры и факты. – М., 2008.С.51. Ищенко Е.П. Особое производство и его связь с противодействием расследованию// Противодействие расследованию и меры по его преодолению: Сб. матер. 51-х криминалистических чтений: В 2-ч ч. - М., 2010. С.98.

состязательности при производстве по уголовным делам, предполагающий возможность осуществления правосудия и без достижения истины [11]. На наш взгляд, не следовало полностью отказываться от принципа объективной истины, являющегося гарантом соблюдения законных прав и интересов всех участников уголовного процесса.

Обратимся в этой связи к анализу соотношения состязательности уголовного процесса с тесно связанным с ним противодействием установлению истины. Поскольку сам законодатель допускает состязание, спор между двумя сторонами – обвинением и защитой, постольку наделяет каждую из них прямо противоположными функциями, а это предполагает противоположность целей и задач. Как известно, «в споре рождается истина». Однако не следует забывать, что бывают разные виды споров. В одних спорящие объединены стремлением установить объективную истину о предмете спора (научные споры). В других случаях, главным для сторон является не достижение истины, а победа над соперником. Именно к такому виду спора можно отнести судебный спор в состязательном уголовном процессе, участники которого помогают суду установить лишь ту истину, которая соответствует интересам обвинения и защиты.

Теперь суд исключен из числа субъектов, ищущих истину, и не должен принимать никаких мер по её установлению. Защита же не заинтересована в установлении истины, ей достаточно поставить под сомнение доводы обвинения. В силу закрепления в уголовно-процессуальном законодательстве распределения бремени доказывания и по существующей конструкции предварительного следствия обязанность формирования доказательственной базы по-прежнему возложена на орган расследования, который осуществляет функцию уголовного преследования, обосновывает и аргументирует вывод о виновности обвиняемого. Таким образом, установление истины как цель доказывания адресована лишь к

[11] Уголовный процесс. Учебник / Под общ. ред. В.М.Лебедева. М., 2004. С.17.

стороне обвинения. Сторона защиты стремится к воспрепятствованию достижению истины.

Защита, представляющая собой функцию подозреваемого, обвиняемого, защитника, направленную на то, чтобы опровергнуть или ослабить подозрение или обвинение, определяется как защита от уголовного преследования. С точки зрения стороны обвинения, такая деятельность фактически представляет собой противодействие установлению истины. Противодействие, поскольку оно направлено на недопущение достижения целей противостоящей стороной, является разновидностью конфликтного поведения, представляя тем самым реальную угрозу достижению задач и целей уголовного процесса.

Создание условий для успешной реализации принципа состязательности требует, по нашему мнению, достижения баланса между правами двух сторон - защиты и обвинения.

Некоторые ученые, основываясь на принципе состязательности сторон и поддерживая идею о существенном расширении прав стороны защиты (подозреваемого и обвиняемого, защитника), предлагают обсудить вопрос о процессуальном разрешении защите вести параллельное расследование [12]. Такая тенденция к защите прав и интересов подозреваемого и обвиняемого по-прежнему придает актуальность вопросу о недостаточной защите прав потерпевшего.

Пока же говорить о балансе прав и обязанностей сторон обвинения и защиты не приходится. При этом на следователя по законодательству Узбекистана, возложены обязанности собирать также и смягчающие вину доказательства. Защитник обязанностей не несет и вправе ходатайствовать об ограничении либо пополнении объема доказательственной базы. Зачастую следователь собирает доказательства, в полной мере известные защитнику, который, не раскрывая своих козырей, готовится к схватке в суде, а в суде защитник действует – «разваливает дело», тогда как следователь отсутствует, его

[12] Мартынчик Е.Г. Адвокатское расследование в уголовном процессе. Теоретико-методологические основы доктрины адвокатского расследования. М., 2009. С.100.

лишь представляет прокурор. Получается, что следователь и защитник поставлены в неравные условия: у следователя - только обязанности, а у адвоката – только права. В настоящее время адвокатами работают бывшие следователи ОВД и прокуратуры, проработавшие в этой должности 15-20, а иногда и более лет. А им противостоят следователи, стаж которых не превышает 5 лет. При таком положении вещей нетрудно «завести следствие» в тупик. Не способствуют качеству следствия такие факторы, как возрастание нагрузки и отток квалифицированных кадров.

Неудивительно, что в силу своей зачастую невысокой профессиональной квалификации именно как защитников, адвокаты озабочены в первую очередь поисками не истины, а упущений, пробелов, ошибок следствия, доказательством не истины, а того, что она не установлена обвинением. Деятельность таких защитников по компрометации доказательств обвинения Р.С.Белкин справедливо сравнивал с ролью «санитаров судопроизводства», поскольку зачастую неполнота предварительного следствия, процессуальные упущения и ошибки создают благоприятную почву для успешного «разваливания дела» в суде [13]. По делам в отношении ОПФ функции защитников не ограничиваются рамками их полномочий, определенных законом. Некоторые защитники находятся на постоянном денежном содержании ОПФ и сознательно злоупотребляют своим служебным положением, стремясь, во что бы то ни стало, любою ценой «спасти» подзащитного от уголовного преследования. К тому же общеизвестно, что чем чаще адвокат достигает успеха [14] в своей работе, тем громче «имя» данного адвоката и выше размер гонорара. Налицо преобладание материального фактора, детерминирующего успешную адвокатскую деятельность, над моральными детерминантами, связанными с достижением успеха благодаря профессиональному мастерству в пределах правовых и этических норм. При наличии таких «соблазнов» деятельность защитника, противоречащая закону и

[13] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.,2001. С.195-202.

[14] Здесь и в последующем имеется ввиду как успех адвокатской миссии, осуществляемой в рамках закона и адвокатской этики, так и результат «разваливания дела» с нарушением норм закона и этики.

адвокатской этике, в подобной ситуации мотивируется не столько стремлением оказать юридическую помощь, сколько целью «развалить дело» ради получения больших гонораров.

Создание условий для успешной реализации принципа состязательности требует, по нашему мнению, достижения максимального баланса между правами, как стороны защиты, так и обвинения. Укрепление и расширение гарантий института защиты по уголовным делам нельзя отрывать от усиления требований к самим защитникам, требований моральной безупречности и чистоты, соблюдения законности и адвокатской этики в их деятельности. Однако все вышеназванные способы противодействия, как правомерные, так и преступные, совершались и ранее, когда уголовный процесс не считался состязательным, в рамках права на защиту от обвинения или с нарушением этих рамок.

Состязание между собой сторон уголовного процесса представляет по своему содержанию выражение одной из объективных закономерностей борьбы двух противоположностей, нашедший свое закрепление в УПК Узбекистана в виде принципа состязательности сторон, который сам по себе уже предлагает спор, конфликт, вызванный противоположностью целей и интересов обвинения и защиты. При отсутствии противоположных целей и интересов не мог бы существовать и сам принцип состязательности сторон. Равно как и состязательность сама по себе предполагает противоборствование, противодействие состязающихся сторон в реализации каждой из них своей уголовно-процессуальной функции [15].

Содержание уголовно-процессуальных функций обвинения и защиты в целом не подверглось существенному изменению, если не считать, что суд исключен из числа субъектов, ищущих истину, и не должен принимать никаких мер по её установлению. Состязательный тип уголовного процесса предопределил изменение статуса суда: «превращение его из органа орудия репрессий и

[15] Баев М.О., Баев О.Я. Противодействие адвоката уголовному преследованию подзащитного (Процессуальная неизбежность и пределы допустимого) // Расследование и противодействие ему в состязательном уголовном судопроизводстве: процессуальные и криминалистические вопросы: Сб. науч. трудов. - М., 2007. С.36.

карательного аппарата в прошлом в подлинно независимый институт государства, призванный надежно охранять и защищать права и свободы человека и гражданина» [16].

Так каким на самом деле был уголовный процесс ранее? В различные исторические периоды одни и те же общественные отношения регулируются с помощью различных правовых средств воздействия. Любой учебник советского уголовного процесса или советской криминалистики до 1991 года, если вспомнить, содержал в числе других принцип партийности науки, свидетельствовавший о проникновении государственной идеологии и в науку. Стало быть, противоположность интересов обвинения и защиты обусловливала в какой-то мере состязательность и прежнего уголовного процесса, не считавшегося состязательным, но, как бы мы его не называли, фактически являвшимся таковым по своей природе и содержанию, и в котором судебная власть по форме своей организации выступала средством достижения публичных интересов государства.

Имплементация состязательности сторон в уголовный процесс Узбекистана, таким образом, позволила привести, наконец, форму (тип) уголовного процесса в соответствие с его реальным содержанием – состязательностью, обусловленной противоположностью интересов обвинения и защиты, с одной стороны, и высвободить науку от господства над ней любой, в том числе государственной идеологии, с другой. Выражаясь простым языком, «вещи названы своими именами».

Таким образом, событие преступления по своей природе всегда находилось и будет находиться в фокусе противоборствующих интересов. Уголовный процесс неизбежно сопровождался и будет сопровождаться противодействием установлению истины, независимо от того, провозглашен он по форме состязательным или нет.

---

[16] Каримов И.А. Доклад Президента Республики Узбекистан Ислама Каримова на совместном заседании Законодательной палаты и Сената Олий Мажлиса Республики Узбекистан // -Народное слово от 13 ноября 2010 г. №220.

Реализация принципа состязательности сторон в уголовном судопроизводстве Узбекистана, и это отмечают отечественные и зарубежные исследователи, свидетельствует о высокой степени имплементации международных норм в национальное законодательство. Вот почему это стало одним из наиболее приоритетных направлений судебно-правовой реформы в Республике Узбекистан.

Васин Д.Д.

Особенности проведения предварительного исследования электронных носителей информации при производстве речеведческих судебных экспертиз

Теория судебной экспертизы предусматривает четкий алгоритм действий в рамках судебного исследования, с выделением и разделением стадий[17]:

1. Подготовительная.
2. Аналитическая.
3. Сравнительная.
4. Оценочная.

На исследование, проводимое в рамках таких речеведческих экспертиз, как фоноскопическая и лингвистическая экспертизы все чаще поступают объекты, содержащиеся не на аналоговых носителях, а на электронных. Электронные носители информации можно условно разделить на несколько типов:

1. Внешние и встроенные накопители на жестких магнитных дисках.
2. Карты памяти (флеш-память) различных форматов.
3. Оптические диски.

Родовая определенность речеведческих экспертиз представляет их объект в виде звучащей речи (фоноскопическая), текста (лингвистическая). В силу специфики задач, а именно, извлечения информации, зафиксированной в

[17] Россинская Е.Р., Галяшина Е.И., Зинин А.М. Теория судебной экспертизы / под ред. Е.Р. Россинской, М., 2013

электронной форме на носителе информации для проведения конкретного вида экспертных исследований, экспертам требуются определенные знания в сфере компьютерно-технических исследований. В ст. 4, 8, 16 ФЗ «о ГСЭД»[18] говорится о том, что судебный эксперт обязан провести полное исследование представленных ему объектов и материалов дела, дать обоснованное и объективное заключение по поставленным перед ним вопросам на строго научной и практической основе, в пределах соответствующей специальности, всесторонне и в полном объеме с использованием современных достижений науки и техники. Основываясь на данных о том, что процесс компьютеризации проник так или иначе во все сферы деятельности общества, можно сказать, что существует объективная необходимость на основании знаний, относящихся к сфере судебной компьютерно-технической экспертизы составить необходимый и достаточный алгоритм, оформленный в виде рекомендательной методики описания электронных носителей информации, доступный для применения экспертами других специальностей.

Особенности описания внешнего вида электронного носителя информации и его технических характеристик выходит за пределы компетенции экспертов-лингвистов. Так, например, анализируя ГОСТ 28376-89[19] и судебную экспертную практику можно выявить ряд идентификационных признакам диска такие как:

- номер вокруг центрального отверстия
- номер на информационной поверхности/на этикетке диска
- рукописный и печатный текст на этикетке диска
- цвет, форм-фактор диска.

Необходимость описания носителя информации отвечает следующим требованиям: отождествление поступившего носителя в будущем, с целью пресечения возможности его подмены, либо исследования некорректного объекта, также описание топологии представленных на исследование файлов и их свойств

[18] Федеральный закон от 31.05.2001 N 73-ФЗ (ред. от 08.03.2015) "О государственной судебно-экспертной деятельности в Российской Федерации

[19] ГОСТ 28376-89 «Компакт-диск. Параметры и размеры».

позволяет отразить факт того, что в них не были привнесены сторонние изменения, что в совокупности можно рассматривать как экспертную профилактическую задачу, а также работу над пресечением преступлений коррупционной направленности.

Существует позиция, в соответствии с которой, учитывая изменчивость электронных объектов, содержащиеся в них письменные доказательства должны быть зафиксированы с помощью специалист в области компьютерных или интернет-технологий и предоставлены экспертам в электронном виде[20]. В соответствии с методикой эксперт в том числе на подготовительной стадии при знакомстве с поступившими объектами осуществляет в случае необходимости техническую подготовку объекта к исследованию, однако это осложняется отсутствием единой терминологии в рамках одного класса (рода) экспертиз.

В настоящее время при Росстандарте только начал работу технический комитет по стандартизации «Судебная экспертиза», на базе которого предполагается разрабатывать международные и национальные стандарты, в том числе «Судебная компьютерно-техническая экспертиза. Термины и определения». Данный стандарт облегчил бы работу по унификации и созданию универсального алгоритма описания электронных носителей информации.

Алгоритм должен основываться на криминалистической идентификации и включать перечень признаков, включенных в идентификационное поле, что позволит существенно повысить его эффективность. Также должны быть включены особенности работы с носителями, так как существует шанс изменить имеющуюся на них информации некомпетентным специалистом. Например, изменение данных на оптических дисках, с возможностью перезаписи. Тем самым предлагается разработка универсального понятийного аппарата применимого в современных условиях ко всем экспертизам.

Костикова Н.А.
к.ю.н., доцент

[20] Методика проведения психолого-лингвистической экспертизы материалов по делам, связанным с противодействием экстремизму и терроризму / Кукушкина О.В., Сафонова Ю.А., Секераж Т.Н. М.: ФБУ РФЦСЭ при Минюсте России, 2014

Возможности использования информации с электронного носителя видеорегистратора при расследовании преступлений

В век информационных технологий расследование преступлений практически невозможно представить без использования информации с электронных носителей, на которых могут быть отражены различные сведения, представляющие интерес для следователя.

В частности, на таких носителях могут быть обнаружены:

- специальное программное обеспечение, использовавшееся при совершении противоправных действий, вредоносные компьютерные программы;
- сведения о незаконных финансовых операциях;
- информация, запрещенная законом к распространению;
- электронная корреспонденция участников преступления;
- сведения, составляющие различные виды тайны либо нарушающие авторские и смежные права;
- иная информация[21].

Как видно из приведенного перечня, электронные носители достаточно информативны, но содержащиеся на них данные первоначально должны быть извлечены и изучены с целью определения их значимости для конкретного уголовного дела. Для грамотного осуществления данной работы необходимо понимать, что подразумевается под электронным носителем, какие их виды существуют и как правильно изъять такой объект.

В УПК РФ, несмотря на неоднократное упоминание об электронных носителях (ст.ст. 81, 82, 166, 182 и 183), не содержится понятия таковых. Не вдаваясь в научную дискуссию, отметим, что электронный носитель – это

[21] Осипенко А.Л., Гайдин А.И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 156.

материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники[22].

Основываясь на данном понятии, А.Б. Судницын выделяет несколько видов электронных носителей, а именно: внутренний накопитель на жестком магнитном диске (жесткий диск, винчестер, Hard Disk Drive – HDD); оптический диск (лазерный диск, компакт-диск, CD, DVD, диск Blu-ray, HD-DVD); флеш-память (Compactflash, Memory Stick, micro-SD и др.); гибкий магнитный диск (дискета, Floppy Disk Drive – FDD) и многие другие, в том числе микросхема памяти (интегральная схема, чип, микрочип), которая может реализовывать функции миникомпьютера[23].

Большинство современных электронных цифровых устройств оснащено различными видами электронных носителей. Например, в видеорегистраторе в зависимости от его конструктивных особенностей могут использоваться жесткие диски или карты флеш-памяти.

Видеорегистратор, являясь устройством, предназначенным для записи, хранения и воспроизведения видеоинформации, может использоваться в качестве элемента системы наблюдения на стационарных (например, в частных домах, торговых точках, офисных зданиях) и подвижных (например, автомобилях) объектах. При этом целевое назначение видеорегистратора зависит от места его установки.

Так, автомобильный видеорегистратор чаще всего используется для разрешения спорных ситуаций на дорогах, особенно при дорожно-транспортных преступлениях. Примером может служить уголовное дело в отношении Г., который управляя личным автомобилем, допустил наезд на Ш., причинив ему телесные повреждения, повлекшие смерть. Одним из доказательств по делу выступала скопированная на DVD-диск видеозапись с видеорегистратора,

[22] ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения (введен в действие Приказом Росстандарта № 1628-ст от 22.11.2013). М.: Стандартинформ, 2014. С. 2.

[23] Судницын А.Б. Отдельные процессуальные и организационные особенности изъятия и хранения электронных носителей информации при производстве по уголовным делам // Вестник Сибирского юридического института ФСКН России. 2016. № 1 (22). С. 12.

установленного в автомобиле Г. Указанная запись позволила не только установить обстоятельства дорожно-транспортного происшествия, но и полностью опровергнуть показания Г., ссылавшегося на невозможность видеть пешехода из-за стоявшего справа автомобиля. Кроме того, видеофонограмма, изученная в совокупности с другими материалами дела экспертом – автотехником, позволила определить наличие технической возможности предотвращения наезда на пешехода[24].

Однако не исключено, что с помощью видеорегистратора будет зафиксирована не связанная с дорожным движением информация. Так, факт хищения ювелирных изделий из салона-магазина и признаки внешности подозреваемого П. оказались зафиксированными видеорегистратором, установленным в автомобиле свидетеля Ю. Изъятые с видеорегистратора видеофайлы способствовали установлению обстоятельств совершенного грабежа, а также опознанию П. продавцом ювелирного магазина[25].

Приведенные примеры наглядно подтверждают, что информация, отраженная на электронном носителе видеорегистратора, важна для расследования преступлений. Однако для придания доказательственного значения содержащимся на конкретном носителе сведениям, сам носитель должен быть надлежащим образом приобщен к материалам уголовного дела.

Изъятые в ходе осмотра, выемки или обыска электронные носители информации, по мнению исследователей, могут рассматриваться в качестве вещественных доказательств или иных документов.

Рассматриваемые объекты Л.Б. Краснова безоговорочно относит к вещественным доказательствам, поскольку имеющие отношение к делу данные содержатся во внешних признаках (намагничивание определенных секторов диска); они могут служить средством обнаружения преступления, установления фактических обстоятельств дела, выявления виновных либо опровержения

[24] Приговор Кировского районного суда города Красноярска по делу № 1-397/2015 [Электронный ресурс]. URL: http://sudact.ru/ (дата обращения: 28.04.2016).
[25] Приговор Бавлинского городского суда Республики Татарстан по делу № 1-20/2016 [Электронный ресурс]. URL: http://sudact.ru/ (дата обращения: 29.04.2016).

обвинения; в них имеется материальный способ получения, сохранения и передачи невербальной информации[26].

Данный подход оспаривается И.С. Федотовым и П.Г. Смагиным, указывающими, что для процесса расследования представляет интерес не сам предмет, а информация, зафиксированная на носителе и являющаяся, по сути, электронным документом. Это обстоятельство побудило их отнести электронные носители информации к «иным документам»[27].

На наш взгляд, оба подхода имеют право на существование, но практика идет по пути признания электронных носителей информации вещественными доказательствами. Так, по уголовному делу в отношении Х., обвиняемого в покушении на дачу взятки, в качестве вещественного доказательства фигурировала флеш-карта, изъятая из установленного в автомобиле сотрудников ГИБДД видеорегистратора[28]. Изученная в ходе следствия видео- и аудиоинформация, нашедшая отражение на электронном носителе, способствовала доказыванию факта преступного события в ситуации активного противодействия со стороны обвиняемого Х.

Но чаще к уголовному делу приобщаются не первоисточники информации (например, карта флеш-памяти видеорегистратора), а электронный носитель со скопированной при производстве следственного действия видеоинформацией. Например, при расследовании умышленного причинения средней тяжести вреда здоровью информация с видеорегистратора, установленного в автомобиле потерпевшего П., была скопирована на CD-диск, который и был признан вещественным доказательством. Указанная видеозапись и результаты проведенной фоноскопической экспертизы (проводившейся для установления дословного содержания разговора П. с обвиняемыми Е. и Н.) способствовали

[26] Краснова Л.Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 257 – 258.
[27] Федотов И.С., Смагин П.Г. Электронные носители информации: «вещественные доказательства» или «иные документы»? // Вестник Воронежского государственного университета. 2014. № 3 (18). С. 198.
[28] Приговор Кировского районного суда г. Кемерово по делу № 1-286/2015 [Электронный ресурс]. URL: http://sudact.ru/ (дата обращения: 29.04.2016).

доказыванию преступного события и его участников, а также восстановлению предкриминальной ситуации[29].

Поскольку работа с электронными носителями информации обладает определенной спецификой, высказываются заслуживающие внимания предложения о совершенствовании криминалистической и уголовно-процессуальной науки.

Так, К.Е. Дёмин предлагает выделить криминалистическое исследование электронных носителей информации как отрасль криминалистической техники, изучающую закономерности образования виртуальной следовой картины, а также разрабатывающую средства, приемы и методы их обнаружения, изъятия и исследования в целях раскрытия, расследования и предупреждения преступлений. С содержательной стороны эта отрасль должна включать теоретические положения о принципах конструирования и функционирования компьютерных средств, информационно-телекоммуникационных систем, компьютеризированных радиоэлектронных устройств, различных видах электронных документов[30].

Новым направлением совершенствования российского уголовно-процессуального права, как справедливо отмечает Р.И. Оконенко, могло бы стать введение понятия «электронное доказательство». К числу признаков, наполняющих данное понятие содержанием, он относит:

- способность хранить значительный объем сведений;
- легкость копирования сведений, содержащихся на электронном носителе;
- возможность получения информации, хранящейся как в памяти самого устройства, так и в информационно-телекоммуникационной сети Интернет или в иной коммуникационной системе;

[29] Приговор Ленинского районного суда г. Барнаула Алтайского края по делу № 1-272/2015 [Электронный ресурс]. URL: http://sudact.ru/ (дата обращения: 29.04.2016).
[30] Дёмин К.Е. К вопросу о выделении криминалистического исследования электронных носителей информации как новой отрасли криминалистической техники // Библиотека криминалиста. Научный журнал. М.: Юрлитиформ, 2013. № 5 (10). С. 176 – 177.

– относительность и неочевидность содержания цифровых данных[31].

Реализация указанного предложения может положительно сказаться на правоприменительной практике и прекратить дискуссии об относимости электронных носителей к тому или иному виду доказательств.

В заключении отметим, что современные технические устройства, оснащенные электронными носителями информации, играют важную роль при расследовании преступлений. Как показало проведенное исследование, зафиксированные в памяти видеорегистраторов данные при правильной их оценке позволяют выявить предкриминальные, криминальные, а в некоторых случаях – посткриминальные обстоятельства.

Колотушкин С.М.
д.ю.н., профессор

Обязательное использование видеорегистраторов на автотранспортных средствах как элемент в концепции безопасности дорожного движения.

Президент Российской Федерации В.В. Путин подписал закон, который обязывает суды принимать видеозаписи с авторегистраторов в качестве доказательств при рассмотрении дел о дорожно-транспортных нарушениях. Федеральный закон расширяет возможности лиц, привлекаемых к административной ответственности, по представлению доказательств (например, записи видеорегистратора) в обоснование своей позиции при рассмотрении дел об административных правонарушениях.

Это обусловлено тем, что высокий уровень латентности дорожно-транспортных происшествий (ДТП), когда не ясен круг вопросов, связанных с

[31] Окоменко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3 (52). С. 123.

условиями и механизмом происшествия, становится причиной невозможности их полного расследования. Многие уголовные дела по ДТП приостанавливаются на неопределенный срок. В таких условиях возникает необходимость разработки систем, подобных «черным ящикам» авиационной техники, с помощью которых можно было бы получить информацию относительно условий и механизма дорожно-транспортного происшествия. Это могут быть индивидуальные для каждого транспортного средства системы контроля за его движением. Использование подобных систем могло бы существенно снизить уровень необходимых для расследования ДТП сил и средств и оказывать сдерживающее влияние на нарушения водителями правил дорожного движения.

В данной статье предлагается система объективного контроля, которая является обязательной для всех автотранспортных средств. В ней будет фиксироваться два вида информации – визуальная и звуковая.

Фиксация визуальной и звуковой информации, несомненно, должна производиться в движении и при остановках транспортного средства. Запись информации при остановке или выключении двигателя автомобиля прекращается. Нужно отметить, что нет потребности в постоянной фиксации информации вне условий ДТП, поэтому указанная система предусматривает запись и стирание видео и звуковой информации. Следовательно, записываемая информация через некоторое время начинает стираться, но на любой промежуток времени в буфере памяти остаётся запечатлённая информация последних секунд.

В процессе работы такой системы идут два параллельных процесса: во-первых, это запись информации, а во-вторых, ее стирание. Проведенный анализ уголовной и административной практики расследования ДТП показал, что общее время постоянной фиксации визуальной и звуковой информации может быть около 50 секунд. При этом время распределяется следующим образом: 30 секунд – время, предшествующее ДТП; 5 секунд – время фиксации непосредственно ДТП (например, столкновения); 15 секунд – время после совершенного ДТП.

Далее, если говорить о визуальной информации, то нужно отметить, что эта информация должна фиксировать обстановку на дороге в любых погодных условиях и при любом освещении. Также должны фиксироваться знаки светофоров и световых сигналов автомобилей в любое время дня и ночи на расстоянии не менее 300 метров.

Сектора наблюдения водителем должны быть ориентированы вперёд по направлению движения транспортного средства. Проведённые исследования, говорят о том, что около 80% случаях во время движения в уличных условиях и при движении вне населённых пунктов водитель наблюдает вперёд по направлению движения автомобиля в зоне ограниченной горизонтальным углом $70^0 – 80^0$. Вертикальный угол обзора имеет естественные границы. Для большинства автомобилей вертикальный угол наблюдения составляет не более 55^0.

Проводя различные исследования рассматривалось множество вариантов размещения телекамеры наблюдения. По их итогам, наиболее рациональным местом ее расположения, которое отвечает всем условиям, является кронштейн крепления зеркала заднего вида в салоне. Важным моментом, является то, что данная система контроля должна фиксировать скорость автомобиля, но эти параметры не должны сниматься с показаний спидометра. Следовательно, система объективного контроля не должна быть зависима от состояния и качества работы автомобиля.

На лобовом стекле транспортного средства может располагаться светодиодный маячок, указывающий на наличие и включенность предлагаемой системы объективного контроля.

В перспективной системе для съемки может использоваться любая серийная цифровая видеокамера, имеющая достаточную разрешающую способность и угол обзора. Телекамера и другие элементы системы должны быть предварительно протестированы.

Важным моментом является то, что хранение информации в системе объективного контроля после ДТП не должно требовать дополнительного электропитания. А также особой защите должен быть подвергнут элемент системы, где хранится записанная информация. Блок хранения информации должен быть установлен в самом безопасном месте в салоне автомобиля. Таковым является пространство под задним пассажирским сиденьем, либо между передними сиденьями (водительским и пассажирским).

Установка и проверка системы объективного контроля может осуществляться специалистами при проведении ежегодного технического осмотра автомобиля специализированными, в том числе и страховыми компаниями. Основные блоки системы объективного контроля и его порты после их проверки пломбируются специалистами страховых компаний с отметками в документах автовладельца.

После совершении ДТП жесткий диск вынимается из прочного герметичного корпуса, отсоединяется от каналов поступления визуальной и акустической информации и электросети. При снятии блока фиксируется (составляется документ) с описанием состояния системы контроля, ее номеров, пломб, печатей и других реквизитов. Считывание информации с системы объективного контроля осуществляется путем соединения через соответствующие порты с компьютером подобно флэш-картам.

Таким образом, предлагаемая система контроля за движением транспортного средства являются важным источником объективной информации,

которая может составлять доказательственную базу по конкретному делу. Предлагаемая система может являться гарантом защиты от фальсификации. Качество проведения экспертных исследований при использовании объективной информации позволит в кратчайшие сроки получить квалифицированное объективное заключение относительно причин и условий совершения ДТП.

Предложенная система контроля за движением транспортного средства может изменить ситуацию к снижению аварийности так как, реализует возможность получения объективной информации с места ДТП и, во-вторых, - несет в себе психологический, сдерживающий фактор по соблюдению действующих в настоящее время правил дорожного движения.

Кучин О.С.
д.ю.н., профессор

Виды носителей информации, изучаемые наукой криминалистикой

Носитель информации это физическая среда, непосредственно хранящая информацию. Основным носителем информации для человека является его мозг. Собственную, мозговую память человека можно назвать оперативной памятью. Здесь слово “оперативный” является синонимом слова “быстрый”. Заученные знания воспроизводятся человеком мгновенно. Собственную память еще можно назвать внутренней памятью, поскольку ее носитель – мозг – находится внутри человеческого организма. Носитель информации — строго определённая часть конкретной информационной системы, служащая для промежуточного хранения или передачи информации.

Основа современных информационных технологий – это компьютер (ПК). Когда речь идет о компьютере, то можно говорить о носителях информации, как о внешних запоминающих устройствах (или о внешней памяти). Эти носители информации можно классифицировать по различным признакам, например, по

типу исполнения, материалу, из которого изготовлен носитель и т.п. Список носителей информации не является исчерпывающим. Некоторые носители информации мы рассмотрим более подробно:

1. Ленточные носители информации – это магнитная лента, носитель магнитной записи, представляющий собой тонкую гибкую ленту, состоящую из основы и магнитного рабочего слоя. Рабочие свойства магнитной ленты характеризуются её чувствительностью при записи и искажениями сигнала в процессе записи и воспроизведения. Наиболее широко применяется многослойная магнитная лента с рабочим слоем из игольчатых частиц магнитно-твёрдых порошков гамма-окиси железа (γ-Fe2O3), двуокиси хрома (CrO2) и гамма-окиси железа, модифицированной кобальтом, ориентированных обычно в направлении намагничивания при записи.

2. Дисковые носители информации, к которые относятся к машинным носителям с прямым доступом. Понятие прямой доступ означает, что компьютер может «обратиться» к дорожке, на которой начинается участок с искомой информацией или куда нужно записать новую информацию. Накопители на дисках наиболее разнообразны:

- Накопители на гибких магнитных дисках (НГМД), они же флоппи-диски, они же дискеты
- Накопители на жестких магнитных дисках (НЖМД), они же винчестеры (в народе просто «винты»)
- Накопители на оптических компакт-дисках: CD-ROM (Compact Disk ROM), DVD-ROM

Имеются и другие разновидности дисковых носителей информации, например, магнитооптические диски, но ввиду их малой распространенности мы их рассматривать не будем.

3. Накопители на гибких магнитных дисках (дискеты), некоторое время назад были самым популярным средством передачи информации с компьютера на компьютер, так как интернет в те времена был большой редкостью, компьютерные сети тоже, а устройства для чтения и записи компакт дисков стоили очень дорого. Дискеты и сейчас используются, но уже достаточно редко. В основном для хранения различных ключей (например, при работе с системой клиент-банк) и для передачи различной отчетной информации государственным надзорным службам. Дискета это портативный магнитный носитель информации, используемый для многократной записи и хранения данных сравнительно небольшого объема. Этот вид носителя был особенно распространён в 1970-х — начале 2000-х годов. Вместо термина «дискета» иногда используется аббревиатура ГМД — «гибкий магнитный диск» (соответственно, устройство для работы с дискетами называется НГМД — «накопитель на гибких магнитных дисках», жаргонный вариант — флоповод, флопик, флопарь от английского floppy-disk или вообще "печенюшка"). Обычно дискета представляет собой гибкую пластиковую пластинку, покрытую ферромагнитным слоем, отсюда английское название «floppy disk» («гибкий диск»). Эта пластинка помещается в пластмассовый корпус, защищающий магнитный слой от физических повреждений. Оболочка бывает гибкой или прочной. Запись и считывание дискет осуществляется с помощью специального устройства — дисковод (флоппи-дисковод). Дискета обычно имеет функцию защиты от записи, посредством которой можно предоставить доступ к данным только в режиме чтения. Внешний вид 3,5” дискеты представлен на рис. 1.2.

4. Накопители на жестких магнитных дисках, где в качестве накопителей на жестких магнитных дисках широкое распространение в ПК получили накопители типа «винчестер». Термин «винчестер» возник из жаргонного названия первой модели жесткого диска емкостью 16 КВ (IBM, 1973 г.), имевшего 30 дорожек по 30 секторов, что случайно совпало с калибром 30/30 известного охотничьего ружья «Винчестер».

5. Накопители на оптических дисках, к которым относится: компакт-диск («CD», «Shape CD», «CD-ROM», «КД ПЗУ») — оптический носитель информации в виде диска с отверстием в центре, информация с которого считывается с помощью лазера. Изначально компакт-диск был создан для цифрового хранения аудио (т. н. Audio-CD), однако в настоящее время широко используется как устройство хранения данных широкого назначения (т. н. CD-ROM). Аудио-компакт-диски по формату отличаются от компакт-дисков с данными, и CD-плееры обычно могут воспроизводить только их (на компьютере, конечно, можно прочитать оба вида дисков). Встречаются диски, содержащие как аудиоинформацию, так и данные — их можно и послушать на CD-плеере, и прочитать на компьютере. Оптические диски имеют обычно поликарбонатную или стеклянную термообработанную основу. Рабочий слой оптических дисков изготавливают в виде тончайших плёнок легкоплавких металлов (теллур) или сплавов (теллур-селен, теллур-углерод, теллур-селен-свинец и др.), органических красителей. Информационная поверхность оптических дисков покрыта миллиметровым слоем прочного прозрачного пластика (поликарбоната). В процессе записи и воспроизведения на оптических дисках роль преобразователя сигналов выполняет лазерный луч, сфокусированный на рабочем слое диска в пятно диаметром около 1 мкм. При вращении диска лазерный луч следует вдоль дорожки диска, ширина которой также близка к 1 мкм. Возможность фокусировки луча в пятно малого размера позволяет формировать на диске метки площадью 1-3 мкм. В качестве источника света используются лазеры (аргоновые, гелий-кадмиевые и др.). В результате плотность записи оказывается на несколько порядков выше предела, обеспечиваемого магнитным способом записи. Информационная ёмкость оптического диска достигает 1 Гбайт (при диаметре диска 130 мм) и 2-4 Гбайт (при диаметре 300 мм).

Широкое применение в качестве носителя информации получили также магнитооптические компакт-диски типа RW (Re Writeble). На них запись информации осуществляется магнитной головкой с одновременным

использованием лазерного луча. Лазерный луч нагревает точку на диске, а электромагнит изменяет магнитную ориентацию этой точки. Считывание же производится лазерным лучом меньшей мощности.

Во второй половине 1990-х годов появились новые, весьма перспективные носители документированной информации - цифровые универсальные видеодиски DVD (Digital Versatile Disk) типа DVD-ROM, DVD-RAM, DVD-R с большой ёмкостью (до 17 Гбайт).

По технологии применения оптические, магнитооптические и цифровые компакт-диски делятся на 3 основных класса:

1. Диски с постоянной (нестираемой) информацией (CD-ROM). Это пластиковые компакт-диски диаметром 4,72 дюйма и толщиной 0,05 дюйма. Они изготавливаются с помощью стеклянного диска-оригинала, на который наносится фоторегистрирующий слой. В этом слое лазерная система записи формирует систему питов (меток в виде микроскопических впадин), которая затем переносится на тиражируемые диски-копии. Считывание информации осуществляется также лазерным лучом в оптическом дисководе персонального компьютера. CD-ROM обычно обладают ёмкостью 650 Мбайт и используются для записи цифровых звуковых программ, программного обеспечения для ЭВМ и т.п.;

2. Диски, допускающие однократную запись и многократное воспроизведение сигналов без возможности их стирания (CD-R; CD-WORM - Write-Once, Read-Many - один раз записал, много раз считал). Используются в электронных архивах и банках данных, во внешних накопителях ЭВМ. Они представляют собой основу из прозрачного материала, на которую нанесён рабочий слой;

3. Реверсивные оптические диски, позволяющие многократно записывать, воспроизводить и стирать сигналы (CD-RW; CD-E). Это наиболее универсальные диски, способные заменить магнитные носители практически во всех областях применения. Они аналогичны дискам для однократной записи, но содержат

рабочий слой, в котором физические процессы записи являются обратимыми. Технология изготовления таких дисков сложнее, поэтому они стоят дороже дисков для однократной записи.

В настоящее время оптические (лазерные) диски являются наиболее надёжными материальными носителями документированной информации, записанной цифровым способом. Вместе с тем активно ведутся работы по созданию ещё более компактных носителей информации с использованием так называемых нанотехнологий, работающих с атомами и молекулами. Плотность упаковки элементов, собранных из атомов, в тысячи раз больше, чем в современной микроэлектронике. В результате один компакт-диск, изготовленный по нанотехнологии, может заменить тысячи лазерных дисков.

Все рассмотренные выше носители информации косвенно связаны с электроникой. Однако имеется вид носителей, где информации хранится не на магнитных/оптических дисках, а в микросхемах памяти. Эти микросхемы выполнены по FLASH-технологии, поэтому такие устройства иногда называют FLASH-дисками (в народе просто «флэшка»). Микросхема, как можно догадаться, диском не является. Однако операционные системы носители информации с FLASH-памятью определяют как диск (для удобства пользователя), поэтому название «диск» имеет право на существование.

Флэш-память (англ. Flash-Memory), это разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти. Флэш-память может быть прочитана сколько угодно раз, но писать в такую память можно лишь ограниченное число раз (обычно около 10 тысяч раз). Несмотря на то, что такое ограничение есть, 10 тысяч циклов перезаписи — это намного больше, чем способна выдержать дискета или CD-RW. Стирание происходит участками, поэтому нельзя изменить один бит или байт без перезаписи всего участка (это ограничение относится к самому популярному на сегодня типу флэш-памяти — NAND). Преимуществом флэш-памяти над обычной является её

энергонезависимость, т.е. при выключении энергии содержимое памяти сохраняется. Преимуществом флэш-памяти над жёсткими дисками, CD-ROM-ами, DVD является отсутствие движущихся частей. Поэтому флэш-память более компактна, дешева (с учётом стоимости устройств чтения и записи) и обеспечивает более быстрый доступ.

Хранение информации это способ распространения информации в пространстве и времени. Способ хранения информации зависит от ее носителя (книга — библиотека, картина — музей, фотография — альбом). Этот процесс такой же древний, как и жизнь человеческой цивилизации. Уже в древности человек столкнулся с необходимостью хранения информации: зарубки на деревьях, чтобы не заблудиться во время охоты; счет предметов с помощью камешков, узелков; изображение животных и эпизодов охоты на стенах пещер.

Компьютер предназначен для компактного хранения информации с возможностью быстрого доступа к ней. Информационная система, это хранилище информации, снабженное процедурами ввода, поиска и размещения и выдачи информации. Наличие таких процедур — главная особенность информационных систем, отличающих их от простых скоплений информационных материалов.

Человек по-разному подходит к хранению информации. Все зависит от того сколько ее и как долго ее нужно хранить. Если информации немного ее можно запомнить в уме. Нетрудно запомнить имя своего друга и его фамилию. А если нужно запомнить его номер телефона и домашний адрес мы пользуемся записной книжкой. Когда информация запомнена (сохранена) ее называют данные.

Данные в компьютере имеют различное назначение. Некоторые из них нужны только в течение короткого периода, другие должны храниться длительное время. Вообще говоря, в компьютере есть довольно много «хитрых» устройств, которые предназначены для хранения информации. Например, регистры процессора, регистровая КЭШ-память и т.п. Но большинство «простых смертных» даже не

слышали таких «страшных» слов. Поэтому мы ограничимся рассмотрением оперативной памяти (ОЗУ) и постоянной памяти, к которой относятся уже рассмотренные нами носители информации. В компьютере тоже есть несколько средств для хранения информации. Самый быстрый способ запомнить данные — это записать их в электронные микросхемы. Такая память называется оперативной памятью. Оперативная память состоит из ячеек. В каждой ячейке может храниться один байт данных. У каждой ячейки есть свои адрес. Можно считать, что это как бы номер ячейки, поэтому такие ячейки еще называют адресными ячейками. Когда компьютер отправляет данные на хранение в оперативную память, он запоминает адреса, в которые эти данные помещены. Обращаясь к адресной ячейке, компьютер находит в ней байт данных.

Адресная ячейка оперативной памяти хранит один байт, а поскольку байт состоит из восьми битов, то в ней есть восемь битовых ячеек. Каждая битовая ячейка микросхемы оперативной памяти хранит электрический заряд.

Заряды не могут храниться в ячейках долго — они «стекают». Всего за несколько десятых долей секунды заряд в ячейке уменьшается настолько, что данные утрачиваются.

Для постоянного хранения данных используют носители информации. Компакт диски и дискеты имеют относительно небольшое быстродействие, поэтому большая часть информации, к которой необходим постоянный доступ, хранится на жестком диске. Вся информация на диске хранится в виде файлов. Для управления доступом к информации существует файловая система. Имеется несколько типов файловых систем.

Чтобы данные можно было не только записать на жесткий диск, а потом еще и прочитать, надо точно знать, что и куда было записано. У всех данных должен быть адрес. У каждой книги в библиотеке есть свой зал, стеллаж, полка и инвентарный номер — это как бы ее адрес. По такому адресу книгу можно найти.

Все данные, которые записываются на жесткий диск, тоже должны иметь адрес, иначе их не разыскать.

Структура данных на диске зависит от типа файловой системы. Все файловые системы состоят из структур, необходимых для хранения и управления данными. Эти структуры обычно включают загрузочную запись операционной системы, каталоги и файлы. Файловая система также исполняет три главных функции:

1. Отслеживание занятого и свободного места
2. Поддержка имен каталогов и файлов
3. Отслеживание физического местоположения каждого файла на диске.

Различные файловые системы используются различными операционными системами (ОС). Некоторые ОС могут распознавать только одну файловую систему, в то время как другие ОС могут распознавать несколько. Некоторые из наиболее распространенных файловых систем:

- FAT (File Allocation Table)
- FAT32 (File Allocation Table 32)
- NTFS (New Technology File System)
- HPFS (High Performance File System)
- NetWare File System
- Linux Ext2 и Linux Swap

Файловая система FAT используется DOS, Windows 3.x и Windows 95. Файловая система FAT также доступна в Windows 98/Me/NT/2000 и OS/2. Она реализуется при помощи File Allocation Table (FAT - Таблицы Распределения Файлов) и кластеров. FAT - сердце файловой системы. Для безопасности FAT имеет дубликат, чтобы защитить ее данные от случайного стирания или неисправности. Кластер - самая маленькая единица системы FAT для хранения данных. Один кластер состоит из фиксированного числа секторов диска. В FAT

записано, какие кластеры используются, какие являются свободными, и где файлы расположены в пределах кластеров.

FAT32 - файловая система, которая может использоваться Windows 95 OEM Service Release 2 (версия 4.00.950B), Windows 98, Windows Me и Windows 2000. Однако, DOS, Windows 3.x, Windows NT 3.51/4.0, более ранние версии Windows 95 и OS/2 не распознают FAT32 и не могут загружать или использовать файлы на диске или разделе FAT32. Эта система является развитием файловой системы FAT. Она основана на 32-битовой таблице распределения файлов, более быстрой, чем 16-битовые таблицы, используемые системой FAT. В результате, FAT32 поддерживает диски или разделы намного большего размера (до 2 ТБ).

NTFS (Новая Технология Файловой Системы) доступна только Windows NT/2000. NTFS не рекомендуется использовать на дисках размером менее 400 МБ, потому что она требует много места для структур системы. Центральная структура файловой системы NTFS - это MFT (Master File Table). NTFS сохраняет множество копий критической части таблицы для защиты от неполадок и потери данных.

HPFS (Файловая система с высокой производительностью) это привилегированная файловая система для OS/2, которая также поддерживается старшими версиями Windows NT. В отличие от файловых систем FAT, HPFS сортирует свои каталоги, основываясь на именах файлов. HPFS также использует более эффективную структуру для организации каталога. В результате доступ к файлу часто быстрее и место используется более эффективно, чем с файловой системой FAT. HPFS распределяет данные файла в секторах, а не в кластерах. Чтобы сохранить дорожку, которая имеет секторы или не используется, HPFS организовывает диск или раздел в виде групп по 8 МБ. Такое группирование улучшает производительность, потому что головки чтения/записи не должны возвращаться на нулевую дорожку каждый раз, когда ОС нуждается в доступе к информации о доступном месте или местоположении необходимого файла.

Операционная система Novell NetWare использует файловую систему NetWare, которая была разработана специально для использования службами NetWare.

Файловые системы Linux Ext2 и Linux были разработаны для ОС Linux OS (Версия UNIX для свободно распространения). Файловая система Linux Ext2 поддерживает диск или раздел с максимальным размером 4 ТБ.

Все вышеперечисленные носители информации изучаются наукой криминалистикой как потенциальные следовые носители. Основная проблема стоящая перед криминалистикой заключается в том, чтобы «привязать» любой из носителей и находящуюся в нём информацию к непосредственному её автору или пользователю.

Махтаев М.Ш.

д.ю.н., профессор

Электронные носители информации как объекты криминалистического исследования

Анализ практики расследования преступлений в сфере высоких технологий свидетельствует о том, что в большинстве случаев в качестве доказательств по уголовным делам выступает информация, содержащаяся в электронных носителях информации, изымаемых в ходе проведения следственных осмотров, выемок, обысков, других следственных действий и оперативно-розыскных мероприятий.

В криминалистической и иной специальной литературе нет единого устоявшегося подхода к определению понятия «электронные носители информации», чему в немалой степени способствует и законодатель, который используя в законе термин «электронные носители информации» (ст. 81, 82, 182 и 183 УПК РФ) не разъясняет какие носители информации относятся к электронным, а в ст. 5 УПК РФ не сформулировал самого понятия «электронные

носители информации». Такое положение вынуждает следователей и других практических работников обращаться к иным нормативно-правовым актам для уяснения сущности данного понятия. Так в справке Государственно-правового управления, комментирующей принятие ФЗ № 143, которым внесены изменения в УПК РФ в части уточнения порядка изъятия электронных носителей информации, содержащих сведения о деятельности хозяйствующих субъектов, и возвращения изъятых носителей и (или) копирования содержащейся на них информации[32], в качестве электронных носителей информации названы компьютерные блоки, серверы, ноутбуки и карты памяти. Следует согласиться с Осипенко А.Л. и Гайдиным А.И., которые справедливо полагают, что такой перечень электронных носителей информации не может быть применен в следственной практике[33] и предлагают обратиться к понятию, сформулированному в ГОСТе 2.051-2006: «Электронный носитель – это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники». Однако такое определение также не вносит ясности в отношении круга объектов, относящихся к электронным носителям информации.

Объектами, которые без сомнения подпадают под приведенное определение ГОСТа, по мнению Осипенко А.Л. и Гайдина А.И. являются носители информации, не являющиеся частью другого устройства и реализующие функцию хранения информации в качестве основной. Сюда следует отнести: внешние накопители на жестких магнитных дисках, в том числе подключаемые через интерфейс USB; оптические носители информации (CD, DVD, Blu-ray диски); карты флэш-памяти в различном конструктивном исполнении. При проведении следственных действий в отдельных случаях еще могут быть обнаружены и такие практически вышедшие из употребления носители информации, как дискеты (накопители на гибких магнитных дисках), накопители на магнитной ленте (кассеты стримеров), магнитооптические диски и диски для устройства Zip-drive.

---

[32] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 28.07.2012 г. № 143-ФЗ // Собрание законодательства РФ. – 2012. - № 31. – Ст. 4332.

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

Кроме того, электронными носителями информации являются установленные в средствах вычислительной техники внутренние накопители на жестких магнитных дисках (НЖМД, «винчестеры»). Именно на таких устройствах, входящих в состав серверов компаний и персональных компьютеров сотрудников, наиболее часто находится информация, представляющая особый интерес для следствия[34].

Если придерживаться данного в ГОСТе 2.051-2006 определения, то к электронным носителям информации следует относить все устройства, реализующие функцию записи, хранения и воспроизведения информации. Соответственно, к ним должны быть причислены и широко используемые в различных изделиях интегральные микросхемы памяти. Так называемые устройства или модули памяти – оперативные запоминающие устройства (ОЗУ) и постоянные программируемые запоминающие устройства (ППЗУ) – входят в состав многих современных объектов: лабораторных и офисных приборов, объектов бытовой техники, сувениров, игрушек и др. Электронные устройства памяти присутствуют в современных платежных картах и даже в паспорте гражданина Российской Федерации для хранения биометрических данных его владельца. Как правило, в ППЗУ «прошито» постоянно используемое программное обеспечение либо хранится определенный набор данных, которые могут быть считаны с применением специализированных устройств. В ОЗУ программы или данные загружаются временно и сохраняются в течение сеанса обработки до отключения питания[35].

В последнее время все большее распространение получает хранение больших объёмов компьютерной информации в так называемых облачных хранилищах, расположенных на удаленных сетевых серверах, что необходимо учитывать при поиске криминалистически значимой информации. Необходимо также учитывать, что различными типами карт флэш-памяти оснащены большинство современных электронных цифровых устройств (смартфоны,

[34] См.: Осипенко А.Л., Гайдин А.И. Указанная работа.
[35] Там же.

планшеты, фотоаппараты, электронные книги, медиаплееры, видеорегистраторы и т.п.). Преступники могут умышленно скрывать значимую информацию путем ее записи на флэш-карту, помещенное в устройство, которое данную информацию может не распознавать. Например, висящая на стене фоторамка может иметь карту памяти, на которой, наряду с файлами фотоснимков записаны иные файлы, не воспроизводящиеся данным устройством. Текстовая информация может быть зашифрована или скрытно размещена в файлах иных типов с использованием методов стеганографии[36], для ее выявления потребуется применение алгоритмов криптоанализа[37] и стеганоанализа[38] в лабораторных условиях при проведении специализированных экспертиз[39].

Как справедливо подчеркивают Ищенко Е. и Жуланов В., «особенности функционирования мобильной сотовой связи предоставляют следственным органам дополнительные возможности по раскрытию и расследованию преступлений, при организации и совершении которых она использовалась. Каждый мобильный телефон - это миниатюрная приемо-передающая станция, оснащенная специализированным процессором с необходимым объемом электронной памяти, в которой хранятся служебные данные и информация его владельца (список телефонов и др., в зависимости от модели аппарата).

Мобильные телефоны имеют собственные электронные серийные номера, кодируемые в микрочипе аппарата при его изготовлении. Этот номер указывается

---

[36]Стеганография - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Главная задача сделать так, чтобы человек не подозревал, что внутри передаваемой информации, не представляющей внешне абсолютно никакой ценности, содержится скрытая ценная информация. Тем самым стеганография позволяет передавать секретную информацию через открытые каналы, скрывая сам факт её передачи.

Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

[37] Криптоанализ – это наука о методах получения исходного значения зашифрованной информации без доступа к секретному ключу. Можно сказать, что главной целью криптоанализа является нахождение ключа.

[38] Основная задача стеганоанализа – установление факта присутствия в контейнере скрытой информации.

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

на корпусе телефона под аккумулятором. Каждый владелец мобильного телефона при подключении к сотовым линиям связи получает сим-карту, которая, в свою очередь, содержит сведения, необходимые для аутентификации: мобильный идентификационный номер и алгоритм, с помощью которых подтверждается подлинность абонента.

Наиболее криминалистически значимой представляется персональная биллинговая и коммуникационная информация. Первая содержит сведения о количестве и длительности звонков, осуществленных в местной сети и с использованием функции роуминга (междугородних), и позволяет судить об интенсивности и широте круга общения владельца мобильного телефона. Вторая содержит данные о входящих и исходящих звонках с аппарата, включая номер абонента, дату и время начала соединения, его длительность и др.

Регистрация и долговременное (как правило, не менее 3-х лет) хранение основных параметров всех телефонных соединений, жесткая взаимосвязь абонента и базовой станции, а также технические возможности современных компьютерных средств и систем управления базами данных позволяют весьма оперативно обработать колоссальные объемы биллинговой и коммуникационной информации и получить сведения, облегчающие раскрытие и расследование преступлений»[40].

Согласно закону, информация на электронных носителях может выступать как в роли вещественных доказательств, так и документов. Однако особенность информации, находящейся в системе или сети компьютеров, или иных электронных носителей информации, заключается в том, что для непосредственного ознакомления с ней, осуществления над ней каких-либо действий необходимо наличие как определенных устройств, так и особых способов, и методов, отличающихся от обычного визуального восприятия. Неуловимый характер информации, хранящейся или передаваемой в электронной или магнитной форме, вызывает особые проблемы, так как такая информация не

[40] Жуланов В., Ищенко Е. Анализ информации из электронных баз данных в следственной группе //Законность, 2007. № 4.

видна невооруженным глазом, и увидеть ее при отсутствии специальных знаний, специальных приборов (устройств) и навыков работы с ними очень сложно. Кроме того, такая информация может быть легко подделана или уничтожена. Легкость с которой можно подделать, стереть или перезаписать заново информацию, хранящуюся в компьютере или в других устройствах и электронных носителях, дает «единственную в своем роде возможность уничтожения вещественных доказательств практически бесследно»[41].Таким образом, в логической цепочке «информация – субъект восприятия информации» необходимо наличие промежуточного звена, а именно особой технологии ознакомления, оперирования и исследования такой информации[42], а также особых средств исследования электронных носителей информации. К отдельным из таких средств можно отнести:

1. Блокиратор записи Shadow 2, способный перенаправить все операции записи на свой внутренний диск, тем самым обеспечивая неизменность информации на исследуемом компьютере;

2. Аппаратный блокиратор записи EPOS Write Protector предотвращает случайное или преднамеренное внесение изменений в данные на жестком диске при выполнении работ в процессе расследования преступлений в сфере высоких технологий. Он разработан в соответствии с требованиями последней версии стандарта протокола ATA-8 и работает абсолютно прозрачно для ПК и программного обеспечения, что позволяет эксперту использовать любую необходимую ему в процессе исследования платформу (DOS, Windows, Linux, MacOS, Unix…) и набор экспертного ПО (EnCase, X-Ways Forensics, The Sleuth

[41] См.: Голубовский В.Ю. Проблемы сохранения вещественных доказательств при расследовании компьютерных преступлений //Компьютерная преступность: уголовно-правовые и криминологические аспекты //Государство и право – М., 2000. - № 9. – С. 104. (Цитируется по: Казанцев В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов. Глава 3. Доказательства и процесс доказывания по делам о преступлениях в сфере высоких информационных технологий //Электронный ресурс: http://www.allpravo/ru/library/doc5195p0/instrum5196/print5203/html).

[42] См.: Казанцев В.В. Криминалистическое исследование средств компьютерных технологий и программных продуктов. Глава 3. Доказательства и процесс доказывания по делам о преступлениях в сфере высоких информационных технологий //Электронный ресурс: http://www.allpravo/ru/library/doc5195p0/instrum5196/print5203/html

Kit…). Небольшие размеры и вес позволяют работать с блокиратором, как в условиях лаборатории, так и на выезде;

3. Программный комплекс для проведения компьютерных экспертиз и исследования электронных носителей информации X-Ways Forensics. Позволяет оперативно решать практически весь спектр задач компьютерной экспертизы и расследования киберпреступлений, от съема данных до составления отчетов. Комплекс не требует инсталляции и может запускаться на любом компьютере под управлением Windows, в том числе и с флэш накопителей. Это дает возможность применять его для быстрого съема и анализа данных при работе вне лаборатории;

4. Портативный криминалистический накопитель Massive Portable Forensic Storage, позволяет хранить до 8 ТБ (терабайт)[43] цифровых улик. Перевозка и обработка большого количества исследуемых дисков может привести к нарушению их целостности. Накопитель расширяет емкость Forensic Dossier и позволяет записать до 8 Тб данных в одном удобном, безопасном и портативном устройстве. Это универсальное решение также совместимо с Logicube NETConnect для подключения к исследуемым данным, хранящимся в накопителе;

5. Дубликатор Talon Enhanced разработан специально для цифровой судебной экспертизы для использования в лаборатории или на выезде и обеспечивает быстрое копирование на скорости более чем 7 Гб/мин, имеет повышенную прочность и идеально подходит для использования в полевых условиях, в том числе в районах, где проводятся военные действия. Простой в установке и легкий в использовании даже для пользователей без технического образования;

6. EPOS FlashExtractor – устройство для восстановления информации с систем хранения данных на основе Flash памяти типа NAND, основанное на технологии физического доступа к Flash памяти. Комплекс позволяет получить доступ к содержимой памяти микросхем NAND Flash в случаях, когда данные

[43] Терабайт (Тбайт, ТБ) — единица измерения количества информации, равная 1 099 511 627 776 (2′40) стандартным (8-битным) байтам или 1024 гигабайтам.

недоступны через штатный интерфейс (накопитель имеет механические или электрические повреждения платы, разрушен транслятор и т.п.);

7. Мобильная лаборатория RoadMASSter-3 предназначена для извлечения, дублирования и анализа информации. Она позволяет быстро и надежно создавать образ и проводить анализ данных. Эта компьютерная система спроектирована для работы в полевых условиях с такими интерфейсами как FireWire 1394A/B, USB, IDE, SATA, SAS и SCSI. RoadMASSter-3 является мощным и универсальным инструментом для эксперта-криминалиста благодаря поддержке различных типов медиа носителей, нескольким методам извлечения информации с возможностью хеширования и мощным процессором для проведения анализа;

8. Программа для судебных экспертов Forensic Toolkit (FTK). Инструмент предназначен для восстановления паролей и дешифрования файлов. Кроме того, в данный продукт включены и другие уникальные разработки: dtSearch - технология, осуществляющая индексирование исследуемой информации и позволяющая проводить настраиваемый, многофункциональный, контекстный поиск; Stellent's Outside In Viewer Technology - технология, позволяющая просматривать файлы более чем 270 различных форматов; Known File Filter (KFF) может использоваться для сортировки исследуемой информации по категориям. Это позволяет эксперту оперативно отделить файлы, не представляющие криминалистический интерес, и обратить свое внимание на файлы, которые содержат криминалистически значимую информацию. FTK– программный продукт, позволяющий провести полное исследование компьютера в рамках судебной экспертизы[44].

Какие бы совершенные средства исследования компьютерной техники и электронных носителей информации на вооружении не были, к их осмотру, изъятию и выемке следователь привлекает квалифицированного специалиста, заранее убедившись в

[44] Более подробно см.: Средства исследования электронных носителей информации //Электронный ресурс: info@bnti.ru. (Техника для спецслужб. Бюро научно-технической информации).

его компетентности. В качестве понятых также привлекаются лица, хотя бы частично сведущие в компьютерных технологиях[45].

Информация в электронном виде (на электронных носителях информации) наряду с компонентами компьютерной техники является одним из объектов, которые могут быть представлены на экспертизу.

При этом, как справедливо полагают Осипенко А.Л. и Гайдин А.И., может быть обнаружены: специальное программное обеспечение, использовавшееся при совершении противоправных действий, позволяющее, например, получить доступ к чужим банковским счетам и кредитным картам, а также вредоносные программы; сведения о незаконных бухгалтерских и финансовых операциях, произведенных в кредитно-финансовой сфере: данные о счетах и картах потерпевших, с которых производились переводы на счета преступников, и отчеты о выполненных денежных перечислениях; информация запрещенная законом к распространению (экстремистские материалы, материалы с детской порнографией и др.); электронная корреспонденция участников преступления, касающаяся его организации и исполнения, сведения о связях преступников и используемых средствах коммуникации, о распределении ролей в преступных группах и планируемых преступлениях; сведения, составляющие государственную, коммерческую, банковскую тайну, а также нарушающие авторские и смежные права; иная криминалистически значимая информация[46].

Наиболее полное, на наш взгляд, представление о значении криминалистического исследования электронных носителей информации дают проводимые в рамках расследования уголовных дел о хищениях с использованием платежных карт судебные экспертизы (исследования специалистов).

---

[45] О тактических особенностях осмотра и изъятия средств компьютерной техники и электронных носителей цифровой информации уже есть довольно обширная литература, в связи с чем мы не будем на этом останавливаться.

[46] См.: Осипенко А.Л., Гайдин А.И. Указанная работа.

В процессе такого расследования возникает необходимость в производстве ряда судебных экспертиз и получении заключений специалистов[47].

Технико-криминалистическая экспертиза платежных карт и слипов позволяет установить: соответствуют ли расположение и содержание реквизитов карты требованиям стандартов для данного типа карт; каковы способы нанесения основного изображения и реквизитов карты; соответствуют ли способы нанесения изображений и содержание реквизитов исследуемой карты способам нанесения изображений и содержанию реквизитов на представленном образце и др.

В случае изъятия платежной карты при необходимости установления ее подлинности на разрешение экспертизы целесообразно поставить следующие вопросы:

- Соответствует ли представленная на исследование платежная карта по способу изготовления и качеству воспроизведения полиграфических реквизитов аналогичной продукции платежных систем (VISA, MasterCard и др.)?
- Каким способом изготовлена платежная карта либо ее часть?

Если в ходе осмотра места происшествия или выемки изъяты слипы[48] и есть в наличии платежная карта, то для закрепления факта ее покупки необходимо поставить следующий вопрос:

- Прокатаны ли слипы с платежной карты, представленной на экспертизу?

При проверке версии о совершении подозреваемым хищений с использованием пластиковых карт неоднократно на разрешение эксперту целесообразно поставить следующие вопросы:

- Прокатаны ли слипы с одной платежной карты или с разных карт?
- На одном или разных импринтерах[49] выполнены оттиски клише предприятия на слипах?

[47] При изложении возможностей судебных экспертиз, проводимых в рамках расследования уголовных дел о хищениях с использованием платежных карт использованы материалы из книги: Настольная книга следователя – СПБ: «Юридический центр Пресс», 2008.

[48] Слип – документ, оформляемый при осуществлении покупки с помощью банковской платёжной карты.

В случаях изъятия оборудования, использовавшегося для изготовления карт, с помощью технико-криминалистического исследования документов возможно установить оборудование, применявшееся при изготовлении карт (эмбоссер[50], печатные формы, использованные для выполнения фонового рисунка и банковских реквизитов, и др.); с помощью трасологического исследования возможно установить оборудование, использовавшееся для вырубки карты, и т. п.

Если карта содержит магнитную полосу, то целесообразно назначение судебной компьютерно-технической экспертизы, целью которой является установление содержания информации на первой, и(или) второй, и(или) третьей дорожках магнитной полосы. Наиболее эффективно назначение комплексной судебной компьютерно-технической и технико-криминалистической экспертизы. Такое исследование дополнительно может установить, соответствует ли данная информация содержимому реквизитов, имеющихся на исследуемой карте. На разрешение компьютерно-технической экспертизы пластиковых платежных карт могут быть поставлены следующие вопросы:

- Какая информация содержится на магнитной полосе пластиковой карты, представленной на исследование?
- Какая информация содержится в памяти микропроцессора, представленного на исследование?
- Подвергалась ли информация, содержащаяся на магнитной полосе (в памяти микропроцессора), несанкционированному изменению?
- Какие данные (файлы) были стерты (уничтожены), скопированы, изменены (модифицированы)?
- Как изменялось их содержание, дата создания (уничтожения, изменения)?

---

[49] Импринтер (англ. *imprinter*) – механическое устройство, предназначенное для оформления слипа при совершении операции с платёжной картой. В импринтер вставляется клише, на котором эмбоссированы идентификационные данные точки приёма. Пластиковую карту вставляют в импринтер и вкладывают слип. На слипе остаётся оттиск идентификационных данных точки приёма и карты клиента.

[50] Эмбоссирование (от англ. *Embossing – тиснение, чеканка*) – процесс механического выдавливания на листовом материале различной информации (придание объема рисунками и надписям). Например, для банковских карт это: номер карты, срок действия, фамилия и имя клиента, название компании (для корпоративных клиентов). Для выдавливания используются специальные устройства – эмбоссеры (англ. *embosser*).

- Существует ли причинно-следственная связь между имевшими место манипуляциями с компьютерной информацией, имеющейся в памяти микропроцессора платежной карты, и изменением функций программного обеспечения банкомата (например, в случае, когда преступникам после перепрограммирования микропроцессора карты удается получить в банкомате деньги в сумме, значительно превышающей остаток на счете держателя карты)?

Вопросы, решаемые при производстве компьютерно-технической экспертизы платежной карты, содержащей чип-модуль, зависят от типа чип-модуля, информации, заносимой в чип-модуль эмитентом, обстоятельств и механизма совершения преступления, возможностей конкретного экспертного подразделения. Если в технологической цепочке по изготовлению карты использовалась ЭВМ, то при проведении компьютерного исследования можно установить, имеется ли на компьютере соответствующая информация (программы для управления устройствами, файлы, содержащие информацию об изготовлении карт, текстовую или графическую информацию, относящуюся либо, возможно относящуюся к их изготовлению).

Изъятые по уголовному делу поддельные пластиковые карты после производства технико-криминалистической экспертизы документов целесообразно направлять для производства экспертизы полимерных материалов и изделий из них (химической), задачами которой является установление:

- состава материала, из которого изготовлена карта, состава красящих веществ, нанесенных на карту;
- типа и вида изделий из полимерных материалов, их торговой марки, предприятия изготовителя;
- факта изготовления изделий на одном предприятии, одном и том же комплекте технологического оборудования, из одной партии сырья, одним способом, по одному технологическому режиму переработки, в одной

партии готовой продукции, хранения и эксплуатации в одних и тех же специфических условиях;

- причин и условий видоизменения тех или иных их качеств в зависимости от внешних воздействий (механических, термических, химических), связанных с обстоятельствами данного события.

При этом следователю необходимо учитывать, что заготовки для изготовления пластиковых карт находятся в свободной продаже и их кустарное изготовление нерентабельно.

Для разрешения вопросов: учинена ли подпись на слипе, пластиковой карте, других документах держателем карты; имела ли место имитация подписи держателя карты; учинена ли подпись подозреваемым лицом; других вопросов относительно авторства выполненных рукописных текстов назначается и проводится судебная почерковедческая экспертиза.

Таким образом, при исследовании поддельных карт может потребоваться достаточно широкий круг специальных знаний. Постановка вопросов, выносимых на исследование, зависит как от вида преступления, способа его совершения, обстоятельств, подлежащих доказыванию, так и от самих исследуемых объектов. Учесть все эти обстоятельства, оценить возможности конкретных видов исследований и правильно сформулировать вопросы следователю может помочь соответствующий специалист в ходе предварительной консультации.

Полстовалов О.В.
д.ю.н., профессор

Об использовании ИТК-технологий в целях оптимизации уголовного судопроизводства: криминалистические и процессуальные аспекты

Современная уголовно-процессуальная наука и криминалистика оказались весьма консервативными по отношению к более широкому, а порой и единственно целесообразному использованию информационно-телекоммуникационных технологий (ИТК-технологий) в уголовном

судопроизводстве. Криминалистика как призванная стоять в авангарде внедрения новых технологий оптимизации досудебного и судебного производства по уголовному делу наука всякий раз должна соотносить внедряемые ею рационализаторские предложения с требованиями о допустимости доказательств. По справедливому утверждению О.С.Кучина, разрабатываемые криминалистикой рекомендации «могут применяться в практической деятельности следователей только при условии, если они подчинены задачам уголовного судопроизводства и непосредственно отвечают принципам и нормам уголовного процесса»[51]. Поэтому при всей внешней привлекательности электронного уголовного правосудия и очевидных преимуществ от внедрения его в реальную действительность практики расследования и разрешения дела по существу налицо объективные сложности для более активного использования ИТК-технологий в максимально возможном объеме на уровне лучших зарубежных стандартов. Одновременно традиционализм, косность и ничем не оправданная инертность законодателей, правоприменителей и консервативно настроенных ученых позволяют лишь дозировано, в небольшом объеме преодолевать стереотипы и предубеждения на пути подобных прогрессивных идей. Обычно все рассуждения с аргументацией «против» опираются на расхожее: что хорошо и применяется в зарубежных странах в большом объеме порой малопригодно или вовсе пагубно для российского правосудия. Поэтому, думается, необходимо построить немалую часть аргументации на имеющихся положительных примерах «в параллельной реальности» отечественного гражданского судопроизводства и ряда административных процедур при осуществлении публичных функций.

Электронный документооборот становится постепенно неотъемлемой частью во всех сферах оказания государственных услуг, к числу которых, без сомнения, можно в полной мере отнести и уголовное правосудие. Электронный формат общения с чиновником минимизирует коррупционные риски, позволяет

[51] Кучин О.С. О необходимости использования в уголовном процессе криминалистических разработок // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства. Материалы международной научно-практической конференции. Отв. ред. А.А. Протасевич. Иркутск: Изд-во: Байкальский государственный университет, 2014. С. 295.

контролировать и проверять добросовестность и компетентность при исполнении своих обязанностей государственным служащим, способствует существенному удешевлению и большей оперативности работы государственного аппарата, что не нельзя не принимать в расчет в контексте современной доминанты восстановительного характера уголовного правосудия. Однако в настоящее время отмечается рост бумажной бюрократии в практике уголовного преследования и рассмотрения уголовного дела в суде. Более того, пустое и никчемное в вопросах надлежащего отправления публичных функций в уголовном процессе бумаготворчество занимает существенную часть рабочего времени следователей, дознавателей, прокуроров и судей. К сожалению, объемы уголовных дел только растут, а качество расследования и рассмотрения дела в суде если и повышается, то не особо заметно, если не принимать за чистую монету бравурные комментарии функционеров от правоохранительных органов о запредельном удельном весе обвинительных приговоров как объективном и адекватном действительности показателе профессионализма и добросовестности решения задач предварительного расследования, а обратиться к практике в столь непопулярном сегодня ЕСПЧ. Вообще бюрократизация по существу выступает прямой противоположностью демократизации, но, тем не менее, бумаготворчество ради бумаготворчества в настоящее время становится настоящей бедой везде и всюду. Поэтому снижение хотя бы сугубо технической нагрузки за счет более широкого использования ИТК-технологий, несомненно, позволит повысить как минимум оперативность работы и снизить затратность досудебного и судебного производства по делу, сделать его более прозрачным для участников процесса, которые в таком формате смогут легче и быстрее знакомится с материалами уголовного дела, заявлять ходатайства и жалобы, т.е. на качественно ином уровне защищать свои права и законные интересы. Разумеется, такой подход должен снизить уровень коррумпированности и формализма, заставить должностных лиц органов уголовного преследования и суда работать более эффективно и по существу.

Глобальная цель создания электронного уголовного правосудия и расширения сферы приложения в этом направлении криминалистических рекомендаций не настолько труднодостижима. «Модернизация уголовного судопроизводства … , – пишут О.В.Качалова и Ю.А.Цветков, – должна вестись одновременно в двух направлениях: во-первых, в направлении внедрения новых информационных технологий, способствующих повышению открытости, доступности и оперативности правосудия, а во-вторых, в направлении усовершенствования самого процесса посредством снижения его избыточного формализма. Одним из универсальных инструментов модернизации уголовного судопроизводства, способствующих одновременному достижению обеих целей, может стать переход от бумажного к электронному уголовному делу»[52]. Законодатель не торопится с внедрением электронного документооборота в полном масштабе в уголовное судопроизводство. Однако 8 марта 2015 года произошло знаковое событие: в УПК РФ появилась первая норма об использовании усиленной цифровой подписи. Положения ч. 2 ст. 393 УПК РФ были дополнены предложением следующего содержания: «Исполнительный лист вместе с копией приговора может направляться судом для исполнения судебному приставу-исполнителю в форме электронного документа, подписанного судьей усиленной квалифицированной электронной подписью в порядке, установленном законодательством Российской Федерации»[53]. Первая ласточка пока не стала общей тенденцией, но по существу именно эта новелла может стать сигналом для более широкого внедрения в практику организации документооборота в уголовном судопроизводстве на основе визирования электронных документов усиленной цифровой подписью. Формальных препятствий к этому нет: как известно, Правила использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, утвержденные

[52] Качалова О.В., Цветков Ю.А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2. С. 95. С. 95 – 101.
[53] Федеральный закон от 8 марта 2015 г. № 41-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Справочно-правовая система «Гарант».

Постановлением Правительства РФ от 9 февраля 2012 г. № 111, не применяются только к отношениям, возникающим при осуществлении обмена электронными документами, содержащими сведения, составляющие государственную тайну (п. 1 указанных Правил)[54]. Поэтому для более широкого использования электронного документооборота не требуется в принципе изменений и дополнений в УПК РФ по каждому частному случаю. Просто необходимо реализовать все необходимые и предусмотренные Федеральным законом «Об электронной подписи»[55] мероприятия, провести соответствующее обучение следователей, дознавателей, прокуроров, судей и работающих в государственных экспертных учреждениях экспертов по работе в таком формате и имеющееся правило сделать общей практикой. Для криминалистов же здесь отрывается по истине «целинные земли» совершенно нового формата организации расследования, взаимодействия следователя с оперативными подразделениями и экспертными службами. Для практики преференции преимущественно будут сводиться к удешевлению и ускорению работы. Представим себе ситуацию, когда следователь назначает производство экспертизы в другом городе и по почте направляет постановление и материалы для ее производства в экспертную организацию, за неимением таковой, к примеру, в г. Уфе. Нередко в Республике Башкортостан необходимость в этом возникает, когда следует установить характер воздействия на организм внеперечневого аналога наркотического вещества, а по этому направлению экспертными возможностями экспертно-криминалистический отдел УФСКН России по РБ не располагает. Поэтому направление постановления и материалов (да еще и не по почте с нарочным) в экспертно-криминалистический отдел УФСКН России по Пермскому краю, где подобные исследования проводятся

[54] Постановление Правительства РФ от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» // Собрание законодательства Российской Федерации от 20 февраля 2012 г. № 8 ст. 1027.

[55] В соответствии со ст. 1 Федерального закона «Об электронной подписи» данный нормативный правовой акт «регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами» (См.: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации от 11 апреля 2011 г. № 15 ст. 2036).

давно и успешно, стало традиционной практикой. Здесь, разумеется, электронным документооборотом ситуацию не разрешить. Однако при направлении уже готового заключения по почте обратно проходит значительное время, что в условиях назначения и производства экспертизы (особенно в стадии возбуждения уголовного дела) имеет принципиальнейшее значение. В действительности эксперты в подобной ситуации могут и по телефону предварительно сообщить необходимую информацию, когда счет идет на часы, но это не меняет ситуацию в корне и следователь вынужден отказывать в возбуждении уголовного дела, когда формально готовое заключение идет почтовым отправлением с положительным (!) для возбуждения уголовного дела результатом. Представляется, что если бы эксперт мог с помощью закрытой электронной сети направить в адрес следователя электронное заверенное усиленной цифровой подписью заключение, то столь драгоценное время для принятия одного из важнейших решений по делу не было бы потеряно. Таких примеров можно назвать не одну сотню, когда необходимость соблюсти процессуальные сроки приводит к принятию содержательно необоснованных, но формально безупречных решений в рамках той информации, которая имеет документальную определенность. Так почему бы не снизить подобные риски расширением возможностей использования во взаимодействии следователей, дознавателей, оперативных и экспертных подразделений электронного документооборота? Тем более, что вся необходимая нормативная база для это имеется.

Электронное правосудие – не фантастическая, а реалистическая и практически безальтернативная перспектива развития уголовного судопроизводства, если таковое всецело будет ориентировано на демократизацию, а не на бюрократизацию. Разумеется, в настоящее время электронная составляющая современного российского правосудия в целом позволила деятельность судов сделать более открытой и прозрачной, но все используемые сервисы в основном носили и носят не определяющий движение

дела, а лишь обеспечительный, сопутствующий характер. В этом смысле науке уголовного процессуального права и криминалистике жизненно необходимо ликвидировать отставание от специалистов, занимающихся схожей проблематикой применительно к гражданскому судопроизводству, где пусть и несистемно, но все же случаются внедрения прорывного характера, а на монографическом уровне развиваются исследования в области электронного правосудия. В частности, В.А.Пономаренко пишет, что «под электронным правосудием следует понимать такой судебно-юрисдикционный порядок рассмотрения гражданских дел, который всецело (включая совершение всех необходимых процессуальных действий) опосредуется электронной формой выражения (закрепления) процессуальной информации и взаимодействия участников гражданского судопроизводства»[56]. Безусловно, для уголовного судопроизводства необходимо принимать за основу и целый ряд поправочных коэффициентов на предмет недопустимости разглашения данных предварительного расследования (ст. 161 УПК РФ), реализации процедур закрытых судебных заседаний (ч. 2 ст. 241 УПК РФ). Однако и эта проблема технически и юридически разрешима, было бы желание. «Внедрение электронного документооборота в судебную систему, – пишет Н.Н.Кухмазова, – необходимо не столько для сокращения временных и материальных издержек в судопроизводстве, сколько в целях обеспечения открытости, прозрачности и доступности правосудия, повышения эффективности работы судебных органов и качества судебных актов»[57]. Для криминалистики же оптимизация в большей оперативности работы имеет принципиально важное значение по вопросу организации и планирования уголовного преследования, а прозрачность и открытость работы органов расследования и судов отвечает по большей части задачам предупреждения коррупции.

Сергеев М.С.

[56] Пономаренко В.А. Электронное гражданское судопроизводство в России: штрихи концепции: монография. М.: Проспект, 2015. С. 11 – 12.
[57] Кухмазова Н.Н. Практика внедрения электронного документооборота в российскую судебную систему // Закон. Февраль 2011. № 2. С. 85 – 86.

Электронная проверка сообщений о преступлении

Вопрос допустимости производства следственных действий и, в частности производства обыска и выемки, на этапе выявления и проверки сообщения о преступления является дискуссионным на протяжении долгого периода времени, но, тем не менее, становится все более актуальным в виду развития технологий, методики расследования, уголовно-процессуального правового регулирования и неоднозначной правоприменительной практики.

Важно отметить, что в настоящее время большинство ученых-процессуалистов обоснованно считают, что на стадии возбуждения уголовного дела имеет место именно доказывание[58]. Полученные же в ходе проверки сообщения о преступлении сведения могут быть использованы в качестве доказательств. По мнению многих правоведов, в виду наделения органов предварительного расследования широкими полномочиями, регламентированными ст. 144 УПК РФ, этап проверки сообщения о преступлении можно рассматривать в качестве неформального расследования[59].

В соответствии со ст. 144 УПК РФ органы и должностные лица, осуществляющие предварительное расследование принимают и проверяют сообщение о совершенном, готовящемся преступлении и принимают решение в пределах компетенции, установленной УПК РФ. В рамках проверки сообщения о преступления дознаватель, орган дознания, следователь, руководитель следственного органа вправе: 1) получать образцы почерка или иные образцы для сравнительного исследования у физических лиц и представителей юридического лица (ст. 202 УПК РФ); 2) получать объяснения; 3) истребовать документы и предметы; 4) изымать документы и предметы; 5) назначать судебную экспертизу; 6) получать заключение эксперта; 6) производить осмотр места происшествия,

[58] Подробнее об этом см.: Кузнецов Н.П. Доказывание в стадии возбуждения уголовного дела. Воронеж, 1983; Быков В.М., Березина Л.В. Доказывание в стадии возбуждения уголовного дела по УПК РФ. Казань, 2006; Сергеев А.В., Овчинникова О.В. Возможность доказывания в стадии возбуждения уголовного дела // Российский следователь. 2009. N 20. С. 15 - 17 и др.

[59] Зажицкий В.И. Дополнения к ст. 144 Уголовно-процессуального кодекса РФ: плюсы и минусы // Российская юстиция. 2013. N 11. С. 28

документов, предметов, трупов; 7) производить освидетельствование; 8) требовать производства документальных проверок, ревизий, исследований, привлекать к участию в этих действиях специалистов; 9) давать органу дознания обязательные для исполнения письменные поручения о проведении оперативно-розыскных мероприятий.

Однако, законодатель, расширив данный перечень следственных мероприятий, не предусмотрел четкий порядок их производства. В связи с чем, на практике возникают проблемы правоприменения, а в литературе возникают споры о законности проведения тех или иных следственных действиях.

Полагаем, что «электронные доказательства» на этапе проверки сообщения о преступлении могут быть получены в результате производства: 1) изъятия документов, предметов; 2) осмотра документов, предметов; 3) оперативных мероприятий; 4) истребование документов, предметов.

Осмотр – это непосредственное обозрение объекта путем его личного восприятия[60]. Главным отличием осмотра документов и предметов от выемки и является то, что при данном следственном действии нельзя применять принуждение.

Оперативные мероприятия – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, осуществляющие оперативно-розыскную деятельность, в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств (ст. 1 ФЗ№ от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности»). В результате применения оперативно-розыскных мер органом дознания иногда получается аудио-, видео-, кинозапись. Согласно позиции Верховного суда носители информации после вовлечения в уголовный процесс

[60] Уголовно-процессуальный кодекс Российской Федерации. Главы 1 - 32.1. Постатейный научно-практический комментарий / Е.К. Антонович, Е.А. Артамонова, Д.П. Великий и др.; отв. ред. Л.А. Воскобитова. М.: Редакция "Российской газеты", 2015. Вып. III - IV. // СПС КонсультантПлюс.

путем производства следственных действий или иных предусмотренных УПК РФ способов собирания доказательств (например, путем представления в порядке ст. 86 УПК РФ) также могут стать доказательством на стадии возбуждения уголовного дела [61].

Истребование документов – действия следователя, дознавателя по направлению предписания гражданину или организации представить определенные материалы, передачу истребуемого объекта и процессуальное оформление этих фактов[62].

Согласно ч.2 ст. 144 УПК, по сообщению о преступлении, распространенной в средствах массовой информации редакция, главный редактор СМИ обязаны передать по требованию лица производящего проверку сообщения о преступлении документы и материалы, подтверждающие сообщение о преступлении, а также данные о лице, предоставившем указанную информацию. Кроме того, ряда преступлений может быть совершен в информационно-телекоммуникационной сети (ст.ст. 137, 159.6, 171.2, 185.3, 228.1, 242, 242.1, 274, 280, 280.1, 282 УК РФ). *Так, например, согласно материалам уголовного дела, установлено, что Кулешовым Е.В. в период с 14 октября 2010 г. по 3 апреля 2013 г. на своей странице в социальной сети «Вконтакте» были размещены видеозаписи экстремистского содержания. 3 апреля 2013 г. следователем в присутствии понятых был осуществлен осмотр сайта сети Интернет – личной страницы сайта «Вконтакте» Кулешова Е.В.. В результате проведенного осмотра на странице были обнаружены 5 видеозаписей предположительно экстремистского содержания. В результате проведенного следственного мероприятия был составлен акт осмотра сайта сети Интернет. Кроме того, было произведено копирование обнаруженных материалов на компакт диск, который был направлен для проведения исследования. В ходе проведенного исследования было установлено, что представленные материалы содержат*

[61] Определения Судебной коллегии по уголовным делам Верховного Суда РФ от 29 декабря 1993 года и от 17 ноября 1994 года // Бюллетень Верховного Суда РФ. 1994. N 11; 1995. N 5.

[62] Артемова В.В. Проблемные аспекты реализации истребования и изъятия предметов и документов на этапе возбуждения уголовного дела // Российский следователь. 2014. N 3. // СПС КонсультантПлюс.

признаки экстремизма. В результате проведенных оперативно-розыскных мероприятий была установлена личность лица, разместившего данные материалы. 25 июня 2013 г. по факту обнаружения в действиях Кулешова Е.В. признаков преступления предусмотренных ч.1 ст. 182 УК РФ составлен рапорт и зарегистрирован в КУСП за №198 от 25.06.2013. Судом полученные доказательства признаны допустимыми и по результатам их исследования, вынесенным 25 октября 2013 г. приговором Кулешов Е.В. признан виновным в совершении преступления, предусмотренного ч. 1 ст. 282 УК РФ[63]. Таким образом, в рамках проверки сообщения о преступления, могут быть использованы «электронные доказательства», а также совершено их копирование. На примере данного уголовного дела, можно сделать вывод о тенденции «электронизации» следственных мероприятий, в частности самостоятельный характер приобретает такое действие как «осмотр сайта». По нашему мнению, осмотра сайта, изъятие электронных носителей информации и копирование информации на данной стадии должно производиться по правилам, установленным п. 9.1 ст. 182 УПК РФ. Обязательным условием проведения таких мероприятий является присутствие специалиста.

Следует отметить тенденцию увеличения количества возбужденных уголовных дел выявленных в результате мониторинга социальных сетей. *Так в социальной сети Periscope 17 ноября была размещена видеозапись, на которой избивают учащуюся одного из учебных заведений г. Казань. Прокуратурой Республики Татарстан по поручению прокурора республики по данному факту была проведена проверка. Согласно материалам видеозаписи установлено, что школьники устроили прямую трансляцию избиения своей одноклассницы на заднем дворе профессионального колледжа №41 в г. Казань. Девочки избивали школьницу, а мальчики снимали это на камеру и комментировали происходящее, нецензурно выражаясь в адрес одноклассницы. По данному факту органом дознания возбуждено уголовное дело по признакам преступления,*

[63] Приговор № 1-795/2013 от 27 сентября 2013 г. [Электронный ресурс] // Архив Ленинского районного суда г. Новосибирска – URL: http://leninsky.nsk.sudrf.ru/ (дата обращения 11.03.2016)

предусмотренного п. «а» ч. 2 ст. 116 УК РФ[64]. Другим примером возбуждения уголовного дела на основании размещенной видеозаписи в социальной сети Periscope стал случай произошедший в ночь с 1 на 2 апреля 2016 г.. *С.Османов, находясь в буддистском храме, осквернил статую Будды. Видеозапись своих действий Османов транслировал в социальной сети Periscope. По результатам изучения данных материалов, по факту осквернения в буддистском храме статуи Будды возбуждено уголовное дело по ст.148 УК РФ*[65]. Также следует отметить рост числа преступлений экстремистского характера, совершенных в сети Интернет. *Так, согласно материалам уголовного дела в период 1 июля по 11 декабря 2014 года Р.Кашапов опубликовал в открытом доступе на своей странице в социальной сети "ВКонтакте" четыре видеозаписи, содержание которых, согласно заключениям экспертов, направлено на нарушение территориальной целостности России и возбуждение межнациональной розни. По результатам проверочных действий было возбуждено уголовное дело по ч. 2 ст. 280.1 и ч.1 ст. 282 УК РФ. Набережночелнинский городской суд РТ, согласившись с мнение государственного обвинителя, признал Р.Кашапова виновным в совершении инкриминируемых ему преступлений*[66].

Министр Внутренних дел РФ В.А. Колокольцев отмечает рост преступлений экстремисткой направленности, совершенной в сети Интернет, так, согласно приведенной статистике: «Всего за 2014 год выявлено 1024 преступления экстремистской направленности, что на 14% превышает показатель 2013 года. Прирост достигнут за счет активизации выявления экстремистских

[64]Прокуратура Татарстана взяла на контроль расследование уголовного дела по факту избиения учащейся казанского колледжа [Электронный ресурс] // Официальный сайт Прокуратуры РТ, 19.11.2015 – URL: http://prokrt.ru/main/news1/prokuratura_tatarstana_vzyala_na_kontrol_rassledovanie_ugolovnogo_dela_po_faktu_izbieniya_sverstnicami_uchawejsya_kazanskogo_kol/ (дата обращения: 12.01.2016)

[65] В Калмыкии возбудили дело об осквернении статуи Будды [Электронный ресурс] // Российская газета, 03.04.2016 http://rg.ru/2016/04/03/reg-ufo/kalmykia-oskverneniia-buddy-vozbudili-delo.html (дата обращения 10.04.2016)

[66] В Набережных Челнах вынесен приговор Рафису Кашапову [Электронный ресурс] // Официальный сайт прокуратуры РФ, 15.09.2015 – URL:http://procrf.ru/news/351768-v-naberejnyih-chelnah-vyinesen.html (дата обращения: 10.04.2016)

направлений в сети интернет - 345 противоправных фактов»[67]

Представляет также интерес другой пример получения «электронных доказательств» в рамках ст. 144 УПК РФ. *Так, 14 декабря 2009 г. в отношении Е. было возбуждено уголовное дело по ч.2 ст. 146, ч. 1 ст. 273 УК РФ. Согласно материалам уголовного дела, Е. 2 ноября 2009 г. с целью извлечения прибыли путем незаконного распространения программных продуктов незаконно скопировал (приобрел) на принадлежащий ему компьютер заведомо нелицензированный, то есть контрафактный, экземпляр не разрешенной к свободному распространению компьютерных программ системы N. стоимостью 216 018 рублей, правообладателем которой является ЗАО N. и хранил его с целью последующего сбыта. На основании имеющейся у правоохранительных органов информации о том, что Е. занимается незаконной установкой и распространением нелицензионного программного обеспечения, было принято решение о проведении оперативно-розыскного мероприятия "проверочная закупка". 5 ноября 2009 г. Е. перевез ноутбук с хранящейся на нем компьютерной программой в здание аэровокзала аэропорта. В ходе проведения оперативного мероприятия «проверочная закупка», установлено, что Е. незаконно сбыл, то есть установил на жесткий диск стационарного компьютера нелицензированный, контрафактный экземпляр компьютерных программ системы N., используя при этом вредоносную программу X., позволяющую обойти процедуру стандартной установки и регистрации информационных баз. В результате преступных действий Е. ЗАО N. причинен ущерб в крупном размере на сумму 216 018 рублей. Полученные видеозапись оперативного мероприятия, протокол проверочной закупки, протокол выемки у Б. телефона с записью разговора с Е. послужили доказательствами по уголовному делу. Также, в ходе осмотра места происшествия у Е. был изъят ноутбук. Судом полученные доказательства признаны допустимыми*[68]. Таким образом, в рамках ст. 144 УПК

[67] МВД РФ отмечает рост количества выявленных экстремистских преступлений в интернете [Электронный ресурс] // Информационное агентство ТАСС 4.03.2015 – URL:http://tass.ru/politika/1807250 (дата обращения 10.04.2016)

[68] Кассационное определение Пермского краевого суда от 12.10.2010 по делу N 22-6934 // СПС Консультант

РФ допустимо изъятие электронных носителей информации, электронной информации, а также проведение «электронного обыска». В материалах уголовного дела указано, что «в ходе осмотра места происшествия, время, установленное на компьютере Б., соответствовало реальному времени у Е.». Иными словами, представляется возможным рассмотрения «электронной среды» в качестве места совершения преступления, в результате чего, возможно выделение понятие «электронный обыск» и «электронное изъятии».

Таким образом, в результате проведенного исследования, можно сделать вывод о целесообразности выделения в качестве самостоятельных следственных мероприятий «электронного осмотра», «электронной выемки (копирования)». Считаем допустимым проведение данных следственных мероприятий на этапе проверки сообщения о преступлении, при соблюдении требований установленных уголовно-процессуального законодательства, в частности при их производстве рекомендуется применения по аналогии ч. 9.1. ст. 182 УПК РФ и ч.3.1. ст. 183 УПК РФ, регламентирующих порядок копирования необходимой информации, а также обязательное участие специалиста.

Халиков А.Н.
д.ю.н., профессор

Использование электронных носителей информации, полученных в результате оперативно-розыскной деятельности в процессе предварительного следствия

В настоящий момент электронные носители информации широко применяются как в криминальной деятельности при совершении практически всех составов преступлений, так и в работе правоохранительных органов, использующих новейшие средства компьютерной и телекоммуникационной аппаратуры для борьбы с преступностью. Однако и в том и в другом случае возникают проблемы о материальном фиксировании носителей электронной формы информации в материалах уголовного дела, что необходимо для доказывания обстоятельств преступления и выполнения иных задач,

предусмотренных уголовным судопроизводством. При этом источником получения различного вида электронных носителей информации, используемых в на предварительном следствии в качестве вещественных и иных доказательств, часто являются результаты проводимых оперативно-розыскных мероприятий. Такими электронными носителями, полученными в ходе оперативной работы являются результаты прослушивания телефонных переговоров, снятие информации с технических каналов связи, средства электронного наблюдения, аудио и видео записи различных ОРМ как опроса, проверочной закупки, оперативного эксперимента и т.д. Кроме этого, органы, осуществляющие оперативно-розыскную деятельность могут изымать различные электронные средства - носители информации, используемые преступниками в качестве орудий преступления, предметов преступления или иных средств, использованных в процессе подготовки, совершения и сокрытия преступлений.

Для того чтобы данные результаты эффективно были использованы при расследовании уголовного дела необходима их квалифицированная легализация, что относится не только к понятию рассекречивания, но и к представлению данной информации в органы предварительного следствия без каких-либо технических и процессуальных изъянов.

Согласно ст. 11 Федерального закона «Об оперативно-розыскной деятельности», представление результатов оперативно-розыскной деятельности органу дознания, следователю, налоговому органу или в суд осуществляется на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, в порядке, предусмотренном ведомственными нормативными актами. В свою очередь в п.п. 16 и 17 Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд от 27 сентября 2013 г. указано, что к передаваемым документам, полученным в процессе оперативно-розыскной деятельности прилагаются (при наличии) полученные (выполненные) при проведении ОРМ материалы фото- и киносъемки, аудио- и видеозаписи и иные носители

информации, а также материальные объекты, которые в соответствии с уголовно-процессуальным законодательством могут быть признаны вещественными доказательствами. В случае необходимости описание индивидуальных признаков указанных материалов, документов и иных объектов может быть изложено в отдельном приложении к сообщению (рапорту). Органом, осуществляющим ОРД, при подготовке и оформлении для передачи уполномоченным должностным лицам (органам) материалов, документов и иных объектов, полученных при проведении ОРМ, должны быть приняты необходимые меры по их сохранности и целостности (защита от деформации, размагничивания, обесцвечивания, стирания и другие). При представлении фонограммы к ней прилагается бумажный носитель записи переговоров. Допускается представление материалов, документов и иных объектов, полученных при проведении ОРМ, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно указывается в сообщении (рапорте) и на бумажном носителе записи переговоров. В этом случае оригиналы материалов, документов и иных объектов, полученных при проведении ОРМ, если они не были в дальнейшем истребованы уполномоченным должностным лицом (органом) хранятся в органе, осуществившем ОРМ, до завершения судебного разбирательства и вступления приговора в законную силу либо до прекращения уголовного дела (уголовного преследования).

Разъясняя указанные положения, Верховный суд РФ в своем Постановлении № 8 от 31 октября 1995 г. «О некоторых вопросах применения судами Конституции РФ при осуществлении правосудия» указал, что результаты оперативно-розыскных мероприятий, связанные «с ограничением конституционного права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также с проникновением в жилище против воли проживающих в нем лиц (кроме случаев, установленных Федеральным законом), могут быть использованы в качестве доказательств по делам, лишь когда они получены по разрешению суда на проведение таких

мероприятий и проверены следственными органами в соответствии с уголовно-процессуальным законодательством» (п. 14). Из указанного Постановления следует, что результаты ОРМ могут быть приобщены к материалам уголовного дела, но силу доказательств приобретают только после их соответствующей проверки и оценки.

Здесь необходимо отметить, что сам термин «результаты ОРД» подразумевает информационную завершенность, суть которой может быть выражена как осмысленные сведения, основанные на собранных, оцененных, истолкованных фактах, изложенных таким образом, откуда ясно их значение для решения какой-либо задачи. Результатами ОРД могут быть итоги одного или нескольких проведенных оперативно-розыскных мероприятий, которые оформлены надлежащим образом (на бумажных, электронных и иных носителях информации) и проверены оперативным путем, а также изъятые документы, предметы или вещества. При этом результаты ОРМ и ОРД отражаются в оперативно-служебных документах (справки, рапорта, акты и т. д.) и, тем самым, заключаются в содержании той информации, которая изложена в оперативных документах. Соответственно, результаты ОРД – это не фактические данные, а только сведения о фактах, то есть источники сведений, которые могут быть подтверждены процессуально[69].

Как известно, результаты оперативно-розыскной деятельности для использования их в качестве доказательств должны пройти три стадии доказывания – *собирание, проверку* и *оценку*. Это относится и к электронным носителям информации, которые в виду специфичности их формы и содержания, с одной стороны, должны содержать относимую к уголовному делу доказательственную информацию, а, с другой стороны, не вызвать сомнения у сторон защиты и обвинения в ее достоверности и допустимости при использовании в качестве доказательств.

[69] Нагиленко Б.Я. О понятии результата оперативно-розыскной деятельности // Оперативник (сыщик). – 2006. – № 4. – С. 21–26; Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К.Горяинова, В.С.Овчинского, Г.К.Синилова. – С. 556–557 и др.

В соответствии с вышеуказанными положениями УПК РФ, ФЗ «Об ОРД» и приведенным судебным комментарием результаты оперативно-розыскной деятельности представляются в уголовный процесс на основании ст. 11 ФЗ об ОРД в соответствующем порядке. После чего данные результаты «принимаются» субъектами уголовного судопроизводства – следователем, органом дознания – на основании ст. 86 УПК РФ, регламентирующей *собирание доказательств* в ходе уголовного судопроизводства путем производства следственных и иных процессуальных действий, т. е. приобщаются к материалам уголовного дела для дальнейшей проверки и оценки. Вместе с тем, следователь, согласно вышеназванной Инструкции, может направить переданные ему результаты ОРД обратно в орган, осуществляющий оперативно-розыскную деятельность, если эти результаты не отвечают требованиям, изложенным в данной Инструкции (п.п.18-20).

Далее в соответствии с общим порядком доказывания в уголовном процессе результаты оперативно-розыскной деятельности *проверяются* на основании ст. 87 УПК РФ путем сопоставления их с другими доказательствами, имеющимися в уголовном деле, установления их источников, получения иных доказательств, подтверждающих или опровергающих результаты ОРД, которые представлены в виде электронных источников информации. С целью проверки переданных органам следствия электронных носителей информации могут быть допрошены оперативные работники и иные лица, участвовавшие в оперативно-розыскных мероприятиях. Основным способом проверки электронных носителей информации являются различного рода экспертизы, которые проводятся с целью исключения монтажа, подделок, установления возможностей для диагностических и идентификационных исследований. В этом случае проводятся фоноскопические экспертизы, экспертизы видеозаписей, компьютерные экспертизы и т.д. Могут производиться и иные следственные действия с целью установления

достоверности сведений, содержащихся в представленных результатах оперативной работы, связанных с электронными носителями информации.

После завершения стадии проверки указанные результаты ОРД подлежат *оценке* в соответствии со ст. 88 УПК РФ с позиций критериев относимости, допустимости, достоверности и достаточности. Иными словами, к результатам ОРД применимы положения уголовного судопроизводства, в соответствии с которыми никакие доказательства (данные) не имеют заранее обусловленной силы, в связи с чем они подлежат проверке и оценке наравне с другими доказательствами по уголовному делу. В целом результаты ОРД, представляемые для использования в доказывании по уголовным делам, должны позволять формировать доказательства, удовлетворяющие требованиям уголовно-процессуального законодательства, предъявляемым к доказательствам в целом, к соответствующим видам доказательств; содержать сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по уголовному делу, указания на ОРМ, при проведении которых получены предполагаемые доказательства, а также данные, позволяющие проверить в условиях уголовного судопроизводства доказательства, сформированные на их основе.

Кроме процессуальных требований к процессу доказывания с применением электронных носителей информации, полученных в результате оперативно-розыскной деятельности, считаем необходимым предложить криминалистические рекомендации с целью эффективного и безошибочного их использования. На наш взгляд, главным в этом случае является, чтобы следователь лично проверил предоставляемые ему сведения на электронных носителях информации, лично сопоставил их с другими данными и доказательствами по уголовному делу и дал свою внутреннюю оценку. Типичной ошибкой следователей является *опосредованный* процесс проверки полученной информации, содержащейся в электронных носителях. После получения результатов ОРД, допустим в виде аудиозаписей прослушивания телефонных переговоров, следователь без личного изучения, личного прослушивания и оформления текста прослушивания

разговоров, направляет все материалы для производства фоноскопической экспертизы. Затем, после получения результатов экспертизы, следователь может формально ознакомить с ее результатами обвиняемого и его защитника и после приобщить эти результаты к уголовному делу. И, наконец, уголовное дело будет направлено в суд, где электронные носители информации подвергнуться тщательному исследованию со стороны представителей защиты и обвинения. И вот тут могут быть различные сюрпризы, как, например, несоответствие фраз на электронных носителях с документальным текстом записи или разговоры, фактически оправдывающие действия подсудимых. Или видеосъемка, заставляющая сомневаться в представленных следствием обстоятельств преступления. Подобные же недостатки могут встретиться и при проверке аудиозаписей, информации, содержащейся в компьютерных базах данных и т.д.

На наш взгляд, отношение к электронным носителям информации, несмотря на их виртуальный характер, их невидимость обычными средствами восприятия, должно быть как к материальным источникам доказывания. Во всяком случае, следователи должны непосредственно проверять и оценивать электронные носители информации, которые в большей части бывают получены в результате оперативно-розыскной деятельности, наравне с другими доказательствами. Причем, в случае определенных сложностей, у следователей всегда есть возможность обратиться к соответствующим специалистам для получения консультаций, разъяснений или, наконец, для определения необходимости назначения соответствующих экспертиз.