ТАКТИКА ОСМОТРА И ВЫЕМКИ НОСИТЕЛЕЙ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

М.В. Старичков
заместитель начальника кафедры криминалистики
ФГКОУ ВПО ВСИ МВД России,
кандидат юридических наук

В статье рассматриваются тактические особенности выемки и осмотра носителей компьютерной информации с учетом современного развития компьютерных технологий.

In the article are considered tactical particularities of withdrawal and check-up of the computer information carriers with provision of modern computer technology development[*].

Рубеж XX-XXI веков ознаменовался бурной эволюцией информационных технологий, повсеместным внедрением средств автоматизированной обработки информации. Однако научно-техническая революция не только обусловливает коренные прогрессивные изменения в общественно-экономических отношениях, но и приводит к появлению новых форм и видов преступных посягательств. Во всем мире отмечается рост «беловоротничковой» преступности – противоправных деяний в сфере высоких технологий, связанных с компьютерными операциями, безналичными деньгами, технологическими секретами, новыми видами мошеннических действий высокообразованных людей[†]. Остропроблемное в плане социальных последствий развитие процессов информатизации общества порождает новое направление в науках криминального цикла, связанное с компьютерной преступностью.

[*] Starichkov M. V. Tactics of the check-up and withdrawal of the computer information carriers.

Соответственно, появился новый криминалистический объект – компьютерная информация, овеществленным представлением которой выступает ее носитель. В подписанном 1 июня 2001 г. в г. Минске Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации компьютерная информация была определена как «информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи». Введенное Федеральным законом от 7 декабря 2012 года № 420-ФЗ примечание 1 к статье 272 Уголовного кодекса РФ, устанавливающее, что «под компьютерной информацией понимаются сведения (сообщения, данные) представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи», не способствует устранению терминологической неопределенности. Поскольку в теории информации и связи сигнал – это физический процесс, параметры которого изменяются во времени в соответствии с передаваемым сообщением, вызывает недоумение, как его можно «хранить».

Понятию «носитель компьютерной информации» («машинный носитель информации») до сих пор не дано легальное толкование, хотя оно неоднократно встречается в различных нормативных актах, в основном ведомственного характера. В какой-то мере раскрыть его сущность представляется возможным с помощью терминов: 1) «носитель информации», под которым понимается а) «физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин»[2] либо б) «гибкие магнитные диски, съемные накопители информации или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и тому подобное, а также распечатки текстовой, графической и иной информации на бумажной или пластиковой основе»[3], и 2) «документ на машинном носителе», т. е. «документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной»[4].

С точки зрения следственной практики машинные носители представляют интерес в качестве источников криминалистически значимой информации, как по делам о высокотехнологичных преступлениях, так и по делам иных категорий (экономических и общеуголовных). На таких носителях могут не только оставаться следы неправомерных манипуляций с компьютерной информацией, но и

содержаться относящиеся к расследуемому событию сведения – переписка, финансовые и иные документы, фото- и видеоматериалы и пр.

Носители компьютерной информации можно классифицировать по различным основаниям, например:

– по физическому способу фиксации информации: на ферромагнитном слое, на микросхемах (CMOS), оптические, на бумажной (пластиковой) основе и др.;

– по возможности перезаписи информации: с однократной записью (лазерные диски CD-ROM и DVD-ROM, перфоленты, перфокарты и т. п.) и перезаписываемые (магнитные диски, сменные карты памяти, флэш-накопители, диски CD-RW и DVD-RW и др.);

– по отношению к компьютерной системе: конструктивно входящие в нее (жесткие магнитные диски, микросхемы постоянного запоминающего устройства (ПЗУ)) и сменные (гибкие магнитные диски, внешние жесткие диски, сменные карты памяти, USB-флэш-накопители, лазерные диски и др.);

– по техническим характеристикам (объему, скорости чтения/записи и др.).

Современные тенденции, направленные на миниатюризацию носителей информации, представляют определенные сложности при их обнаружении. Например, сменные карты памяти размерами 15×11×1 мм (рис. 1) могут быть спрятаны практически в любом малом пространстве.

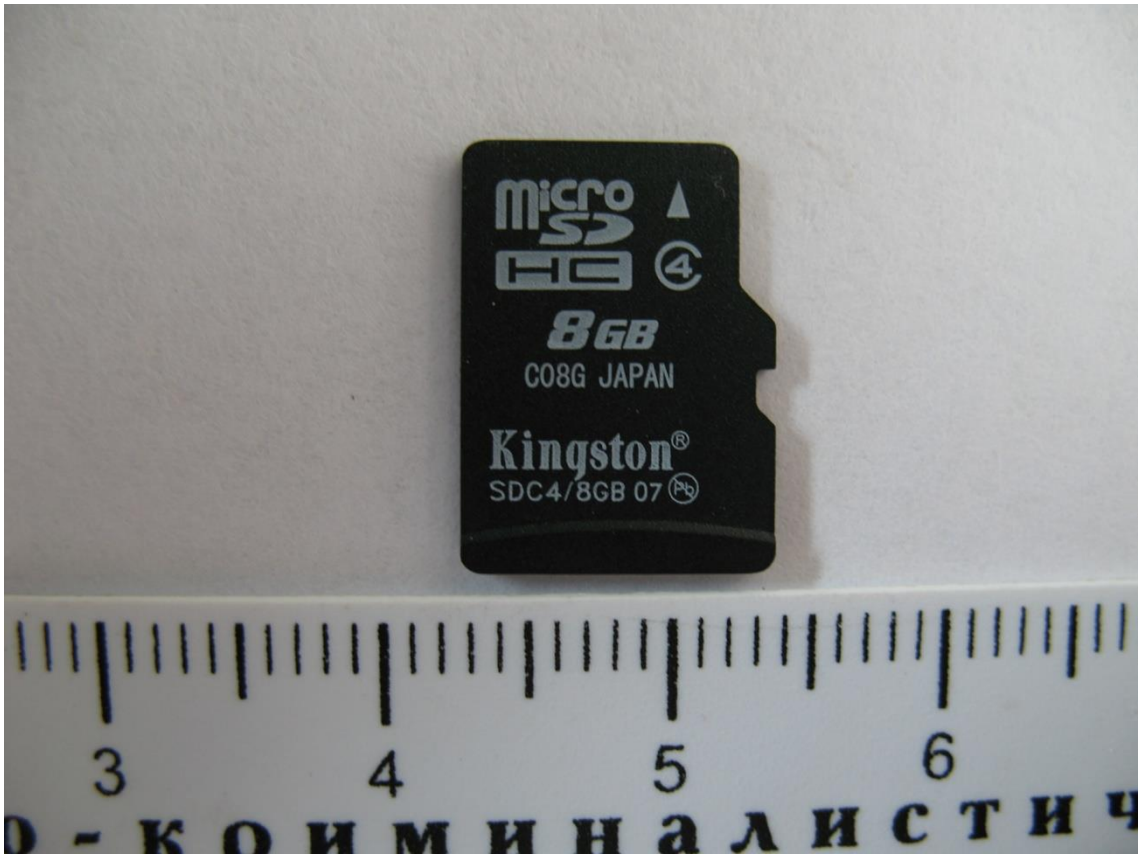

Рис. 1. Сменная карта памяти стандарта MicroSDHC.

Поскольку сильные электромагнитные поля могут повредить хранящуюся на машинных носителях информацию, для их обнаружения нельзя применять активные металлодетекторы, источники рентгеновских и ультрафиолетовых лучей и иные излучающие установки. Сказанное не относится к носителям на бумажной и пластиковой основе, однако для их выявления указанные приборы, как правило, неэффективны.

В настоящее время сотрудникам правоохранительных органов чаще всего приходится иметь дело с персональными компьютерами, используемыми в деятельности различных организаций и в быту. Поэтому типичные носители компьютерной информации – это жесткие магнитные диски (находящиеся в компьютерной системе и внешние), USB-флэш-накопители, сменные карты памяти, оптические диски (CD и DVD). Гибкие магнитные диски (дискеты), активно применяемые еще в начале 2000-х годов и до сих пор упоминаемые в литературе по компьютерным преступлениям, из-за своего малого информационного объема и низкой надежности сейчас практически не используются.

Определить наиболее типичные места сокрытия машинных носителей достаточно сложно, однако их свойства предъявляют определенные требования к их хранению. Практически все носители не переносят высокие (свыше 60°С) температуру и влажность. Носители с ферромагнитным слоем (жесткие и гибкие магнитные диски, магнитные ленты) могут повредиться при отрицательных температурах. Еще большую опасность представляют резкие перепады температур. К неблагоприятным факторам относятся агрессивные химические среды, пыль и сильная вибрация (особенно для жестких магнитных дисков), а также электромагнитное излучение, в том числе прямые солнечные лучи.

Следует помнить, что не только персональные компьютеры и ноутбуки, но и многие современные цифровые устройства – сотовые телефоны, фотоаппараты и видеокамеры, mp3-плееры, фоторамки и др. – также могут выступать в качестве машинных носителей, а находящиеся в них сменные карты памяти нередко содержат информацию, созданную на других устройствах. Кроме того, внешние носители (обычно USB-флэш-накопители) иногда выполняются в виде брелоков, кулонов, авторучек и т. п., что затрудняет определение их функционального назначения.

Изъятие носителей компьютерной информации должно проводиться аккуратно, с соблюдением технических требований, предъявляемых к их

эксплуатации. Часть из них уже была перечислена выше. Нельзя разбирать устройства без предварительной консультации специалиста о безопасности таких действий. Ни в коем случае нельзя прикасаться пальцами и какими-либо предметами, особенно токопроводящими, к разъемам носителей, замыкать контакты. Любое прикосновение к рабочей поверхности оптических дисков может ее загрязнить или поцарапать, что сделает диски нечитаемыми. Их следует брать за боковые края. Изымаются носители по отдельности. Если имеется большое количество однотипных носителей (например, лазерных дисков), допускается их совместное изъятие. При этом упаковка должна обеспечивать их фиксацию, исключающую повреждение при транспортировке и хранении. Хотя современные магнитные носители достаточно стойки к воздействию статического электричества и магнитных полей, все-таки желательно их упаковывать в металлические контейнеры или заворачивать в фольгу. Подписывать упаковку нужно перед тем, как помещать в нее машинный носитель, так как возможно его повреждение при нанесении надписей. Особенно это относится к лазерным дискам.

Осмотр машинных носителей может быть двух видов – внешний и содержащейся на них информации. Внешний осмотр проводится, как правило, на месте при обнаружении и изъятии машинных носителей и сводится к описанию их типа и модели, размера, цвета, комплектности, индивидуальных особенностей – серийного номера, различных надписей, внешних повреждений и т. п. В данном случае можно обойтись без специалиста, однако следователю нужно быть особенно внимательным при использовании специальной терминологии. Так, небольших размеров предметы с USB-разъемом часто называют USB-флэш-накопителями или просто «флэшками». Это может быть действительно так (рис. 2), но подобный внешний вид может иметь и другое оборудование, например Bluetooth-устройство (рис. 3), которое является телекоммуникационным оборудованием, но не машинным носителем. Соответствующие надписи на корпусе от длительного использования иногда стираются, что еще больше затрудняет точное определение типа устройства. Отдельно следует упомянуть внешние USB-картридеры (рис. 4). Сами по себе они не являются носителями компьютерной информации, а лишь устройством для чтения сменных карт памяти, которые могут находиться внутри них. Некоторые модели внешних картридеров дополнительно содержат встроенную память (обычно 1-4 гигабайта), и тогда они тоже будут относиться к машинным носителям. Поэтому при описании таких объектов лучше употреблять общие названия, например «предмет», «USB-устройство».

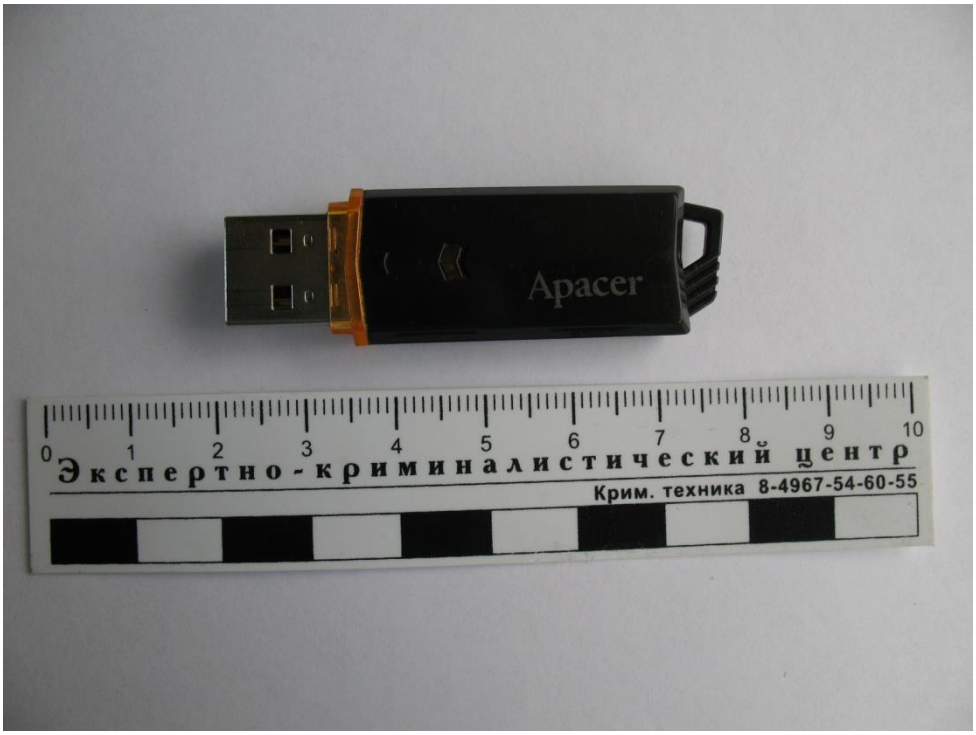

Рис. 2. USB-флэш-накопитель.

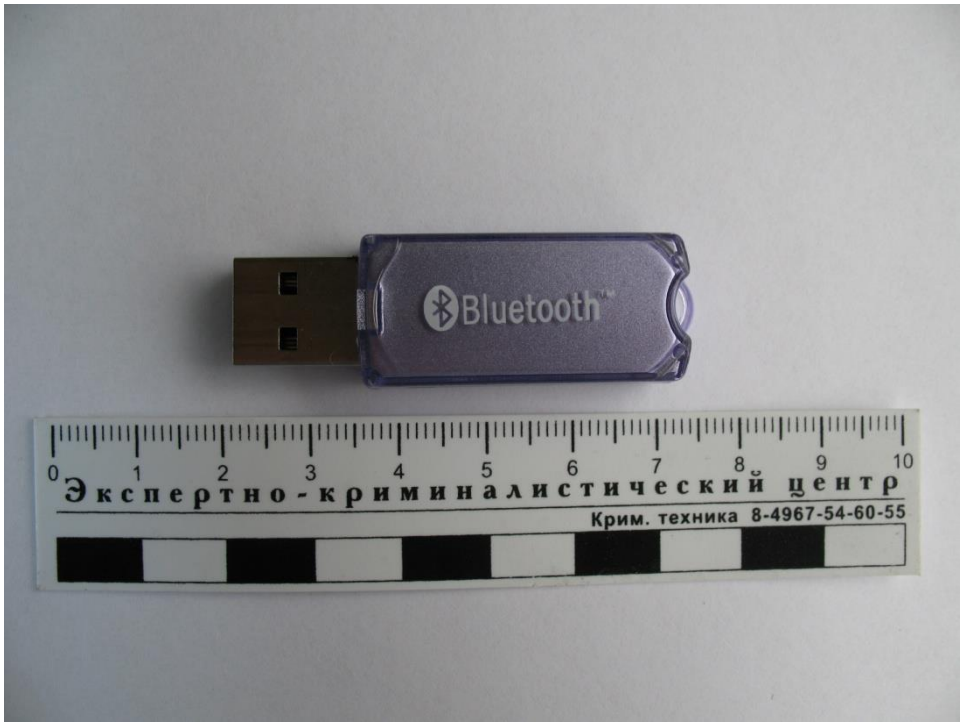

Рис. 3. Bluetooth-устройство.

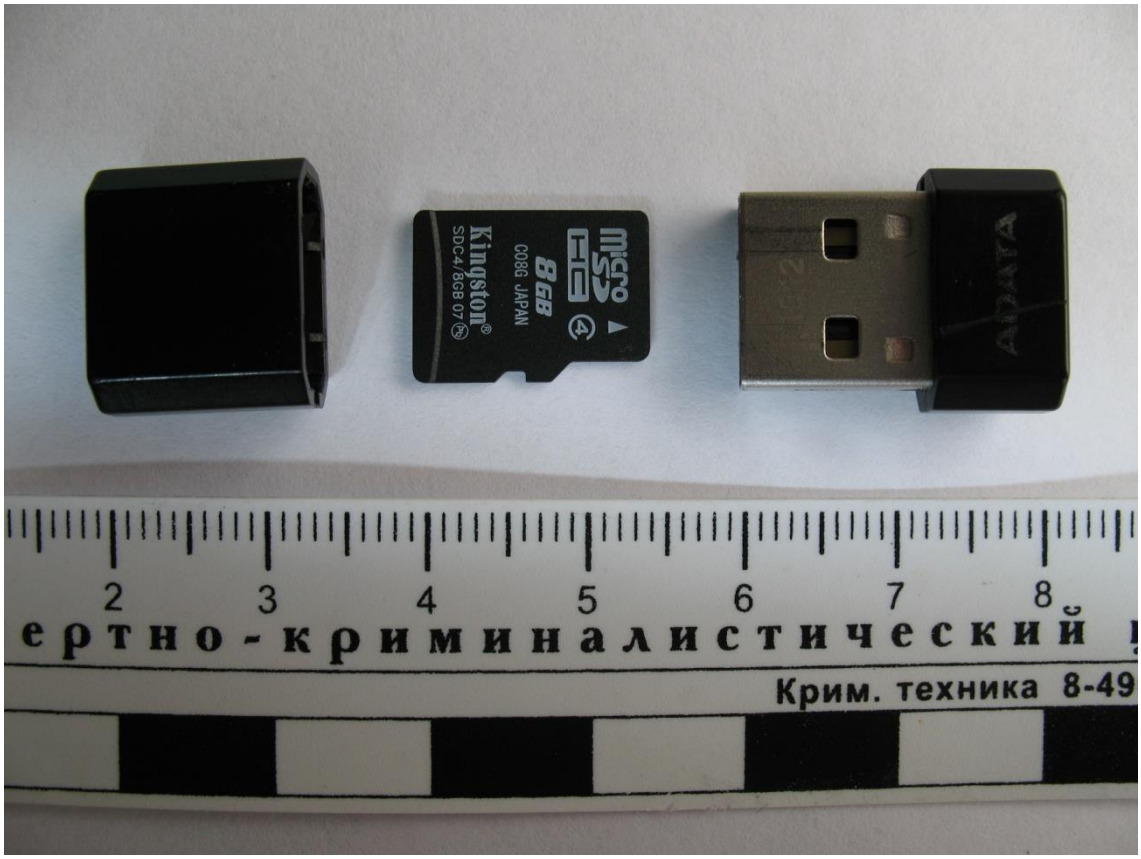

Рис. 4. Внешний USB-картридер стандарта MicroSDHC со сменной картой памяти (в разобранном состоянии)

Разумеется, осмотр проводится в присутствии не менее двух понятых с фиксацией следственного действия в протоколе. Возможно производство фото- или видеосъемки с приложением к протоколу соответствующих фототаблиц или видеозаписи.

Осмотр содержащейся на машинном носителе информации, как правило, требует значительных временных затрат, поэтому обычно проводится в кабинете следователя или, если возникает потребность в специальной аппаратуре, в соответствующем месте (лаборатории). Он должен проводиться с особой осторожностью. Если неумелые действия при просмотре содержимого лазерного диска с вредоносными программами могут привести «только» к уничтожению информации в компьютере, на котором производится осмотр, то другие типы носителей (жесткие магнитные диски, USB-флэш-накопители, сменные карты памяти) сами подвержены изменениям, что влечет утрату криминалистически значимой информации. Поэтому осмотр следует проводить только в присутствии специалиста. В целях обеспечения сохранности доказательств он может создать копию информации, содержащейся на машинном носителе («образ»), и уже с ней проводить дальнейшую работу. Все действия специалиста необходимо подробно фиксировать в протоколе, при этом лучше проводить видеозапись. В необходимых случаях специалист делает копию изображения с экрана монитора («скриншот») и распечатывает ее для приобщения к протоколу.

Таким образом, грамотное производство выемки и осмотра машинных носителей информации требует от лиц, проводящих расследование, наличие определенных познаний в области компьютерных технологий.

ПРИМЕЧАНИЯ

1. Лунеев, В. В. Преступность XX века. Мировые, региональные и российские тенденции / В. В. Лунеев. – М.: НОРМА, 1997. – С. 471.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных / утв. ФСТЭК РФ 15.02.2008.
3. Постановление Центризбиркома РФ от 23.07.2003 № 19/137-4 (ред. от 28.02.2007) «О Положении об обеспечении безопасности информации в Государственной автоматизированной системе Российской Федерации «Выборы»».

Делопроизводство и архивное дело. Термины и определения. ГОСТ Р 51141-98 / утв. Постановлением Госстандарта РФ от 27.02.1998 № 28