

бальная интеграция всех учетов и банков позволит незамедлительно проводить автоматизированный анализ обнаруженных объектов и следов с объектами и следами, имеющимися в информационной системе. В результате будет исключена необходимость перехода из одного банка данных в другой или из одного учета в другой с прохождением каждый раз процедуры авторизации. При реализации глобальной интеграции всех учетов и банков данных получаемая информация действительно станет оперативной и значимой. Реализация логической взаимосвязи компонентов глобальной интегрированной системы позволит повысить информированность каждого сотрудника, предоставит условия для более эффективного использования накопленной информации в процессе расследования, раскрытия и профилактики преступлений. Анализ связей компонентов (следов, объектов и субъектов) системы будет проще, а применение математических алгоритмов (на основе искусственного интеллекта) позволит этот процесс автоматизировать, что во много раз сократит аналитическую работу сотрудников по построению связей.

Информационная безопасность при формировании глобального интегрированного банка данных может обеспечиваться многоуровневой системой защиты, быть подобной имеющимся средствам защиты. Обеспечение информационной безопасности при работе с персональными данными субъектов также может быть организовано имеющимися способами, но дополнено обезличиванием, а именно: пока объекты не будут идентифицированы, вся информация о них будет закодирована. Как только произошла идентификация объектов по заранее определенным признакам, кодировка снимается, в дополнение на служебную почту сотрудника поступает единый код доступа и сотрудник получает полный доступ к информации. Данный способ позволит исключить использование служебной информации в личных целях и будет являться дополнительным уровнем защиты.

УДК 343.985

*А.И. Чурносков, В.В. Тропин*

#### **НЕКОТОРЫЕ ОСОБЕННОСТИ ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

Исследование компьютерной информации является одним из самых молодых направлений в криминалистической технике, которое начало складываться в первой половине 90-х гг. XX в. В настоящее время указанные исследования проводятся почти по всем категориям уголовных

дел. Наиболее часто компьютерная информация исследуется при расследовании преступлений в сфере компьютерной информации; терроризма и экстремизма, экономических и налоговых преступлений; распространения порнографической продукции; преступных нарушений авторских и смежных прав; изготовления поддельной печатной продукции (например, бланков документов, денежных знаков, ценных бумаг). В последние годы значительно выросло число исследований компьютерной информации в ходе раскрытия преступлений против личности. Экспертизы компьютерной информации стали повседневным явлением при рассмотрении как гражданских дел, так и дел об административных правонарушениях.

Компьютерная информация является объектом материального мира, элементом искусственной среды, созданным человеком. Она может существовать только с помощью специальных технических средств – электронно-вычислительной техники и электронных средств связи (систем телекоммуникаций).

Компьютерная информация, как и любой другой вид информации, состоит из двух элементов: содержания (сведения о каком-либо явлении объективной реальности) и материального носителя данных сведений.

Содержание компьютерной информации представлено в форме, пригодной для обработки ЭВМ, ее материальным носителем является электромагнитное поле. В свою очередь, носитель электромагнитного поля может быть материально-фиксированным предметом (жесткий диск, съемные магнитные носители) и не иметь предметной формы (передача информации по беспроводным каналам в компьютерных сетях, например Wi-Fi).

Природа компьютерной информации обуславливает следующие ее свойства, делающие ее весьма сложным объектом криминалистического исследования: компьютерная информация недоступна для непосредственного человеческого восприятия; определенное содержание информации не может быть однозначно закреплено за конкретным материальным носителем; материальный носитель компьютерной информации (электромагнитное поле) невозможно индивидуализировать; содержание информации может быть отделено от ее материального носителя без взаимных изменений; изменение содержания компьютерной информации не вызывает изменений ее носителя, и наоборот; можно быстро обрабатывать, изменять и удалять информацию, в том числе путем удаленного доступа, вне контроля лиц, правомерно пользующихся данной информацией; не всегда возможно восстановить первоначальное содержание измененной или удаленной информации.

Исследование компьютерной информации представляет собой изучение компьютерной информации, полученной при осуществлении оперативно-розыскной деятельности, которое поручается гражданину, обладающему специальными знаниями в науке и технике, в целях получения сведений, необходимых для выполнения задач оперативно-розыскной деятельности.

При проведении исследования компьютерной информации может осуществляться ее копирование.

По результатам исследования компьютерной информации составляется справка.

Объектами исследования являются: персональные компьютеры, планшеты, смартфоны; любые машинные носители информации, периферийные устройства, сетевые аппаратные средства, интегрированные системы, любые комплектующие всех указанных компонентов (аппаратные блоки, машинные носители информации, платы расширения и др.), программы для ЭВМ, алгоритмы, исходные тексты программ, текстовые и графические документы (в электронной форме), изготовленные с использованием компьютерных средств, данные в форматах мультимедиа; информация в форматах баз данных, журналы (протоколы) работы специализированных программ, других приложений прикладного характера.

В предмет исследования компьютерной информации и техники входят: разработка приемов, способов, рекомендаций по обнаружению, фиксации, изъятию и хранению компьютерной информации и техники; изучение состояния и процессов обработки компьютерной информации, состояния и функционирования электронно-вычислительной техники.

Основными методами и средствами исследований являются общие и частные методы математики, радиоэлектроники и информатики, используемые в современных компьютерных технологиях: системный анализ, оптические методы, математическое и имитационное моделирование, топологические методы, инструментальный анализ, метод экспертных оценок и др. В практической деятельности вышеназванные методы реализуются не напрямую, а с помощью широкого набора специальных инструментальных (программных и аппаратных) средств. Например, блокираторы записи, инструменты для получения изображений, копирования, средства документирования, инструменты для поиска и восстановления удаленных файлов, программы для просмотра информации, инструменты для декомпиляции и пошаговой трассировки, различные утилиты и т. д. Привести исчерпывающий перечень указанных средств невозможно в связи с тем, что их арсенал постоянно изменяется вслед за увеличением разнообразия технического и программного обеспечения компьютеров и их систем.

Особое внимание в процессе исследований в связи со спецификой компьютерной информации необходимо уделять требованию ее сохранности в неизменном виде. Соблюдение данного требования обеспечивает возможность проведения повторных и дополнительных исследований. Технически указанный принцип реализуется путем создания точной копии исследуемой информации. Такая копия для последующего производства экспертизы, как правило, создается на дополнительном жестком диске компьютера эксперта (стендовом компьютере). В дальнейшем на нем и выполняются экспертные исследования объектов. При этом основные технические параметры жесткого диска (емкость, среднее время доступа к данным и др.) должны совпадать с параметрами жесткого диска исследуемого компьютера. При невозможности получения резервной копии содержимого жесткого диска должны быть приняты иные меры для сохранности исследуемой информации (например, путем использования программных блокираторов записи).

Все большее распространение получают специализированные программно-аппаратные комплексы. Их использование позволяет получить дополнительную информацию, которую нельзя извлечь при помощи стандартных программных средств, дает дополнительные гарантии неизменности объектов исследования, позволяет облегчить работу сотрудников правоохранительных органов по документальному оформлению соответствующего исследования.

УДК 343.985

*В.Б. Шабанов*

#### **ОРГАНИЗАЦИЯ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ УПРАВЛЕНИЯ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

В теории и практике управления рассматриваются два подхода к управленческой деятельности и организации практических мероприятий – системный (интегрированный) и ситуационный (дифференцированный). Иногда оба подхода используются вместе.

Системой принято считать набор связанных между собой и взаимозависимых элементов (частей целого), которые образуют сложное единство и проявляют определенную временную устойчивость. В этой связи любое подразделение может быть представлено в виде формально организованной, закрытой от посторонних глаз социальной системы, состоящей из отдельных личностей-профессионалов, оргтехники, вспомогательного оборудования, регулярного обмена информацией, т. е. обеспеченной всеми видами необходимых ресурсов. На вход дан-