Инженер по знаниям (специалист, курирующий выбранное направление магистратуры) – сотрудник, который работает с федеральными государственными образовательными стандартами высшего профессионального образования (ФГОС ВПО) и ООП по различным направлениям подготовки. Он наполняет БД СППР информацией о направлениях подготовки и соответствующих им профилях, базовых компетентностных моделях выпускников бакалавриата и магистратуры данного направления, заданных ФГОС ВПО (на рис. 2 $Б_{ФГОС}$ и $М_{ФГОС}$), а также конкретизированных компетентностных моделях, формируемых в рамках реализуемых университетом основных образовательных программ определенного профиля подготовки.

Эксперт (методист) работает совместно с инженером по знаниям. Он определяет и задает новые функциональные связи между компетенциями магистра и бакалавра (М = Б(*f*) на рис. 2), наполняя тем самым БЗ новыми знаниями. Также эксперт участвует в классификации выпускников и распределении по группам в соответствии с их уровнями подготовки на ступени бакалавриата.

ЛПР (документовед) работает непосредственно с выпускниками бакалавриата. Он следит за процессом приема в магистратуру, вводит данные об академических достижениях выпускников из приложений к дипломам и результатах НИРС, а также совместно со студентом принимает решения по определению образовательной программы магистратуры ($М_{ООП}$).

Таким образом, в данной статье предложена концептуальная структура СППР при отборе студентов в магистратуру вуза и ее информационно-функциональная модель, отличающаяся использованием интеллектуальных технологий. Внедрение подобной системы обеспечит повышение качества магистерской подготовки.

Кроме этого создание в крупных учебных заведениях отдела управления магистратурой позволит оптимизировать проведение конкурсного отбора претендентов для обучения на высших образовательных уровнях и повысить эффективность организации их обучения.

Библиографические ссылки

1. *Шарнин В. А.*, *Брусова А. С.*, *Беляева С. В.* К вопросу о необходимости создания Института магистратуры в университете в условиях реформирования высшего образования // Современные наукоемкие технологии. – 2009. – № 2.– С. 5–13.

2. *Лукашенко С. Н.* Развитие исследовательской компетентности студента вуза в условиях многоуровневой подготовки специалистов // Казанский педагогический журнал. – 2010. – № 3. – С.11–18.

E. I. Zakirova, Tchaikovsky branch of Perm National Research Polytechnic University
T. N. Ivanova, PhD in Engineering, Associate Professor, Tchaikovsky branch of Perm National Research Polytechnic University

Information and Analytical Decision Support System as Means of Selection on Master's Programs

Introduction questions in educational process of uniform technology of selection of students for training in a magistracy are considered on the example of creating the information and analysis decision support system (DSS). The designed DSS solves three tasks: classification of bachelors for determining the optimal profile of the master's program, evaluate their level of motivation and individual training results and the distribution of students by groups. The architecture of DSS is given.

Key words: multilevel system of education, competence approach, student selection, decision support system.

УДК 681.5 : 343.98

П. В. Мочагин, кандидат юридических наук, доцент, Удмуртский государственный университет, Ижевск

ИДЕНТИФИКАЦИЯ ВИРТУАЛЬНО-ИНФОРМАЦИОННОГО И НЕВЕРБАЛЬНОГО СЛЕДООБРАЗОВАНИЙ КАК НОВОЕ НАПРАВЛЕНИЕ В КРИМИНАЛИСТИКЕ

Раскрываются понятие и сущность виртуально-информационного и невербального механизма следообразования, его роль при расследовании преступлений.

Ключевые слова: криминалистика, компьютерные преступления, цифровая информация, полиграф, виртуально-информационный и невербально-информационный механизмы следообразования.

История вопроса

На сегодняшний день в криминалистике рассматриваются две формы отражения следообразований – материально фиксированная и идеальная.

Первая форма связана с запечатлением признаков объектов в виде материальных фиксированных следообразований: следы рук, оружия, орудий взлома, подделки документов и т. д.

Получено 04.07.13

Вторая – с мыслительным образом (применительно к жизнедеятельности человека) как результат отражения увиденного объекта (предмета) в сознании человека.

Из общей психологии известно, что образ содержит субъективное отражение объективной действительности и формируется посредством восприятия объекта. Воспринимая объект, человек исследует его, например, обводит взглядом контур объекта при его визуальном восприятии, а значит, действует в отношении объекта. Сказанное справедливо как для процесса формирования образа объекта у очевидца преступления (потерпевшего, свидетеля), так и у лица, совершающего преступление (какое оружие применял, как действовал и т. д.) [1].

Однако в связи с распространением преступлений, совершаемых с использованием цифровых технологий, возникает необходимость введения еще одной формы, которая бы смогла объединить в себе понятие механизма следообразования в виртуально-информацииионной сфере.

С принятием Уголовного кодекса Российской Федерации в 1996 г. введена в действие гл. 28 «Преступления в сфере компьютерной информации», предусматривающая ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, использование программ для несанкционированного уничтожения другой информации и нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации.

То есть если преступник, имея возможность и средства, взломает компьютерную защиту, осуществит неправомерный доступ к компьютерной информации и совершит кражу денежных средств, коммерческой информации, государственной тайны и т. д. виртуальным способом, то он понесет ответственность согласно российскому законодательству. Но возникает вопрос: *как характеризовать форму и механизм такого следообразования, оставленного на месте совершения преступления?*

Если преступник проник тайно в помещение, разобрал корпус компьютера, снял жесткий диск и скрылся, следообразование будет иметь материальный характер. Если преступник подготовил кражу, придумал способ проникновения, разработал план, составил чертежи и передал их для осуществления задуманного, следообразование будет носить идеальный характер.

А если преступник не был на месте совершения преступления физически, а информация с персонального компьютера пропала виртуальным способом или была перекопирована?

Какую форму следообразования преступник в этом случае оставил?

Какая следовая картина будет в этом случае, как идентифицировать такую форму следообразования, если информация крадется с помощью технического устройства, которое позволяет считывать информацию с экрана компьютерного монитора или, как отмечают специалисты, происходит копирование компьютерной информации от руки, путем фотографирования текста с экрана дисплея, что является наказуемым по ст. 272 УК РФ [2].

Определение

На практике получается, что расследования компьютерных преступлений осуществляются, ответственность за данный вид преступления предусмотрена, а четкого определения «компьютерно-техническое следообразование» с точки зрения криминалистической идентификации нет.

Нет и исследований понятий компьютерной информации, ее носителей, механизма образования, формы существования, отграничения компьютерной информации от иных документов и вещественных доказательств с точки зрения уголовно-процессуального законодательства. Еще в 2005 г. И. А. Ефремов обращал внимание на то, что «актуальной проблемой является процессуальное оформление материалов, полученных с применением цифровой аппаратуры» [3].

В криминалистической литературе существует понятие информационных следов, которые отнесены к материально-фиксированным следам. Они обладают рядом особенностей и специфическим источником криминалистически значимой информации – машинным (компьютерным) носителем [4]. Судебные компьютерно-технические экспертизы в зависимости от объекта исследования принято подразделять на компьютерно-технические, программные и сетевые, в которых применяется понятие «информационные следы». Но, учитывая данную классификацию, такой формы определения недостаточно, особенно при идентификации следообразований в случае совершения преступления. Формы отражения следовой информации должны соответствовать, на наш взгляд, форме и механизму следообразования с точки зрения криминалистики.

В связи с этим некоторые ученые криминалисты и практики правоохранительных органов, как и автор этой статьи, основываясь на нововведениях научно-технического прогресса, предлагают дополнить классическую классификацию следов в криминалистике и дифференцировать их в зависимости от их внешнего отображения, принимая во внимание тот факт, что понятие виртуального следообразования представляет собой механизм совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном, виртуальном пространстве компьютерных и иных цифровых устройств, их систем и сетей.

Методические основы

Например, В. А. Мещеряков придерживается идеи формирования так называемых виртуальных следов.[1] Под виртуальными следами он понимает «любое изменение состояния автоматизированной

[1] Понятие виртуального следообразования, представляющего собой механизм совершения любых действий (включения, создания, открывания, активации, внесения изменений, удаления) в информационном виртуальном пространстве компьютерных и иных цифровых устройств, их систем и сетей.

информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами» [5].

Интересную классификацию виртуальных следов предложил А. Волеводз. Одним из оснований для такой классификации может являться непосредственный физический носитель «виртуального следа».

На этом основании он выделяет: 1) следы на жестком диске (винчестере); 2) магнитной ленте (стримере), оптическом диске (CD, DVD); 3) следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ; 4) следы в ОЗУ периферийных устройств (лазерного принтера, например); 5) следы в ОЗУ компьютерных устройств связи и сетевых устройств; 6) следы в проводных, радиооптических и других электромагнитных системах и сетях связи [6].

Семенов А. дополнил классификацию виртуальных следов, подразделив их по месту нахождения на две группы: 1) следы на компьютере преступника; 2) следы на компьютере жертвы. На компьютере жертвы это: а) таблица расширения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы); б) системный реестр операционной системы; в) отдельные кластеры магнитного носителя информации (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации; г) файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы; д) файлы конфигурации программ удаленного соединения компьютера с информационной сетью [7].

Однако А. Волеводз выделил виртуальные следы как непосредственный физический носитель «виртуального следа», а А. Семенов рассмотрел классификацию виртуальных следов с точки зрения их нахождения, но оба автора оставили без внимания форму механизма информационного следообразования, закрепившись изначально на понятии «след».

Краснова Л. предложила классифицировать виртуальные следы по механизму следообразования на первичные и вторичные. Первичные следы, с ее точки зрения, будут являться следствием непосредственного воздействия пользователя с использованием какой-либо информационной технологии, а вторичные – следствием воздействия технологических процессов без участия человека и вне его желания [8]. Но как быть с понятием следообразующего объекта, следовоспринимающего объекта, где в этом случае должен находиться следовой контакт и как он должен классифицироваться?

Некоторые авторы возражают против применения термина «виртуальные следы», мотивируя тем, что «виртуальный» – устоявшийся термин, применяющийся в квантовой теории поля для характеристики частиц, находящихся в промежуточном состоянии или в состоянии неопределенности (координаты которых и сам факт существования в данный момент времени можно назвать лишь с определенной долей вероятности) [9].

В связи с этим В. А. Милашев предложил использовать термин «бинарные следы» как «результаты логических и математических операций с двоичным кодом», но с этим термином опять не согласились [10].

Лыткин Н. Н. отметил, что «изменения в компьютерной информации, являющиеся следами преступления, в подавляющем большинстве случаев доступны восприятию не в виде двоичных кодов (что, собственно, и представляет собой бинарный след), а в преобразованном виде: записи в файле реестра, изменении атрибута файла, электронном почтовом сообщении» [11]. Позже он предложил свой собственный термин «компьютерно-технические следы» [12], но он остался без особого внимания, так как рассматриваемая категория следообразований может оставаться не только в компьютерных, но и в иных цифровых устройствах (в мобильных телефонах и коммуникаторах, цифровых фото- и видеокамерах и т. д.).

Таким образом, можно сделать вывод, что название, которое характеризовало бы следообразование при совершении преступления в «виртуально-цифровом пространстве», предлагаемое разными авторами, так и осталось до конца не сформулированным.

Учитывая необходимость в конкретной идентификации следообразований, которые возникают при совершении преступлений, совершаемых с использованием цифровых информационных технологий, полагаем, что назрела настоятельная необходимость разработки классификации новой формы следообразования – «виртуально-информационной».

Информационная технология

Чтобы обосновать такое название, целесообразно рассмотреть процесс формирования представляемого следообразования, который можно выразить следующим образом.

1. Информация (информационное преобразование). Если исходное состояние объекта обозначить x_1 (компьютер преступника), конечное – x_2 (компьютер жертвы), то преобразование $x_1 - x_2$ будем называть информацией (I) и обозначать $I = x_1x_2$ (информацией владеет преступник и жертва).

2. Код (кодовое преобразование). Преобразование, которое приводит к изменению формы информации в отражательном процессе при неизменности ее содержания, обозначим (K). Например, мысль – ее изложение в письменной форме или с помощью речи.

3. Информирование. Кодовое преобразование информации (I). Например, $I - x_1$ (информация о компьютере преступника) в измененной форме (K) будет $I - x_1 - (K) = I - x_2$ (информация о компьютере преступника преобразована, перекодирована по отношению к информации о компьютере жертвы) [13].

Если (x_1) – компьютер преступника, (x_2) – компьютер жертвы, (I) – информация, содержащаяся в компьютере в момент ее кражи, (t_1) – время изъятия информации, то мы получим: $x_1 = I - (t_1) - x_2$.

Преступник (*P*) владеет информацией (*I*), к примеру, о деньгах жертвы, жертва владеет информацией о количестве собственных средств. Вопрос стоит во времени, когда удобно преступнику (x_1) взломать пароль и проникнуть в систему компьютера жертвы (x_2). В определенный момент времени > t_1 (имеется в виду момент проникновения) информацию компьютера преступника (x_1) преобразуем кодом (*K*) и понимаем, как с помощью сети (*s*) была взломана система компьютера (*y*) жертвы (x_2), получаем: $Px_1 = I - t_1 - (K) = s - y - x_2$. В связи со взломом системы (*s*) в компьютере жертвы (x_2) появляется информация (*I*) о виртуальном проникновении (*V*) в определенный промежуток времени ($t_1 - t_2$) и кражи информации, в нашем случае – денежных средств (*n*). То есть выражению подлежит следующий порядок:

$$Px_1 = I - (t_1 - t_2) - K = s - y - x_2 = V - In.$$

Какое следообразование в этом случаи мы получили?

Было отработано три направления. Первое. Преступник (*P*) физическим путем воздействует на свой компьютер, который выполняет его команды, понятно, что в этом случае механизм следообразования носит материальный характер, но только на начальной стадии. Второе. Команда, отправленная с компьютера преступника, взламывает защиту, другая команда (или их будет несколько) направлена на получение информации и носит виртуальное следообразование (*v*). Третье. Компьютер преступника и компьютер жертвы связаны информационно, то есть задействован код преобразования информации (*K*).

После проведения такой операции компьютер жертвы будет содержать информацию о времени и дате проникновения, какие файлы были открыты, какой объем перекопирован (украден) и т. д.

Компьютер преступника будет содержать всю информацию о незаконном проникновении: 1) различные операции с содержимым памяти компьютера (отображаются в журналах администрирования, журналах безопасности и т. д.); 2) действия с наиболее важными для работы компьютера программами (установка, удаление и т. д.), отражение в реестре компьютера (reg-файлах); 3) сведения о работе в сети Интернет, локальных и иных сетях (аккумулируются в так называемых log-файлах); 4) операции с файлами (отражаются в их свойствах; например, у файлов Microsoft Office в свойствах отражается время создания, последнего открытия, изменения файла и т. д.). В этом случае следообразование будет информационным (*I*).

Таким образом, при совокупности работы и виртуального, и информационного следообразования можно представить третью форму отражения следовой информации как виртуально-информационную (*Vi*). Из этого следует, что, рассматривая данное образование, мы имеем право записать:

$$Px_1 = I - (t_1 - t_2) - (K) - s - y - (x_2 n) = Vi.$$

Это значит, что преступник (*P*) при помощи своего компьютера (x_1) (или другого), владея определенной информацией (*I*), выбрав подходящее время ($t_1 - t_2$), преобразовал в код (*K*), с помощью которого взломал защиту (*s*) по сети (*y*) (в данном случае) компьютера жертвы (x_2) и похитил денежную сумму (*n*), оставив после себя виртуально-информационное следообразование (*Vi*), которое может быть зафиксировано потерпевшим, а в дальнейшем идентифицировано экспертом-криминалистом при расследовании.

Безусловно, в этом случае, говоря о новой форме следообразования (*Vi*), необходимо привести пример из классического механизма следообразования, а именно, когда на первом месте стоит объект следообразующий, затем – следовой контакт и в завершении – объект следовоспринимающий.[2] Данный механизм можно перевести в наш рассматриваемый случай и представить следующей формулой:

$$Px_1(Os_1) = (K) - Vi = (Osv_2)\, x_2,$$

где (Px_1) – преступник, использующий компьютер или другие технические средства, является (Os_1) – объектом следообразующим; (*K*) – код информации, преобразованной в виртуально-информационное следообразование (*Vi*), через которое (Osv_2) – объект следовоспринимающий, (x_2) – компьютер жертвы принимает сигнал и возвращает его обратно тем же путем, но уже с украденной (копированной) информацией (*I*):

$$x_2\,(Osv_2) = Vi - (K) = (Os_1)\, Px_1 = I.$$

Подобное виртуально-информационное следообразование можно найти при работе и с беспроводными технологиями (Интернетом), и при хищении информации с помощью технического устройства, которое позволяет считывать электронно-цифровое отражение с экрана компьютерного монитора, и при записи человеческого голоса за счет электромагнитного поля, состоящего из цифровых значений, на расстоянии и т. д.

Большинство таких виртуально-информационных следообразований могут служить доказательством незаконного проникновения в «память» компьютера или иного устройства (их взлома), доказательством возможного совершения или планирования определенного преступления конкретным лицом или группой лиц.

Таким образом, дальнейшая идентификация новой формы следообразований должна основываться на понимании механизмов преобразования состояний измененных объектов воздействия от начальных к конечным в информационном виртуальном пространстве компьютерных и иных цифровых устройств, их систем и сетей, рассматриваться и идентифицироваться как виртуально-информационные следообразования.

Отталкиваясь от этого определения, можно рассмотреть еще один важный пример проведения пси-

[2] Здесь мы уже не говорим о следовом контакте в трасологическом смысле этого понятия, а представляем следовой контакт в виде виртуально-информационого следообразования.

хофизиологических исследований с применением полиграфа. Процесс достаточно сложен, но заслуживает не меньшего внимания.

У обследуемого, назовем его (*F*), за счет работы зрительной памяти, головного мозга, нервной системы и т. д. сформировалось идеальное следообразование (мы уже говорили о нем выше) по поводу виденья какого-либо события. Сегодня зафиксировать его можно двумя способами: 1) при даче показаний с помощью выражения образов в схемах, графиках, рисунках, то есть интерпретации увиденного, что свойственно в основном глухонемым; 2) при помощи полиграфа, который, в свою очередь, регистрирует психофизиологические реакции (*s*) при работе разного рода датчиков. Возникает вопрос: *какое следообразование получает эксперт в виде полиграммы во время тестирования на полиграфе?*

На обследуемого (*F*) крепятся датчики (*d*), которые позволяют снимать за определенный промежуток времени ($t_1 - t_2$) психофизиологические данные в виде информации идеального следообразования (*Is*), которые в результате кодового преобразования (*K*) фиксирует полиграф (*PL)* в виде графиков – полиграмм.

Таким образом, первоначальную информацию можно записать как

$$F = d - (t_1 - t_2) - (Is) - (K) = PL.$$

Из этого следует, что как только осуществляется регистрация динамики психофизиологических реакций обследуемого лица в ответ на предъявляемые стимулы за счет перевода физиологических показателей активности дыхательной, сердечно-сосудистой системы, электрической активности кожи и других в электрические сигналы, отображаемые в виде графиков, в совокупности образующих полиграмму в виде определенной информации (*I*) и «попадает» в полиграф за определенный промежуток времени ($t_1 - t_2$), механизм следообразования изменится и будет представлять собой виртуально-информационное следообразование (*Vi*), то есть полученные реакции организма, зафиксированные полиграфом, приобретают новую форму следообразования за счет преобразования информации в коды (*K*), которую видит полиграфолог во время тестирования в виде полиграмм на мониторе полиграфа (*M*). Изобразим это преобразование в виде формулы

$$F = I - (t_1 - t_2) - Vi = (K) - M.$$

Учитывая классический механизм следообразования, можно отобразить следующее:

$$I = PL\ (Os_1) = (K) - Vi = (Osv_2) - M.$$

То есть информация (*I*), полученная в процессе полиграфной проверки, будет являться следообразующей (Os_1), за счет кодового преобразования (*K*) будет получен следовой контакт в виде виртуально-информационого следообразования (*Vi*), объектом следовоспринимающим будет являться эксперт-полиграфолог (Osv_2), принимающий информацию на мониторе (*M*).

Остается отметить, что виртуально-информационная форма следообразования остается в полиграфе (так же, как и в случае с компьютером) в виде записанных полиграмм и будет представлять собой доказательственную информацию о проведении психофизиологических исследовании в отношении обследуемого, подозреваемого, свидетеля, подсудимого и т. д.

В завершение следует обратить внимание еще на один вопрос, который связан с невербальной формой следообразования.

Мы уже говорили о том, что на сегодняшний день криминалистика рассматривает две классические формы отражения следообразований – материально фиксированную и идеальную. Нами была предложена еще одна форма – виртуально-информационная.

Настало время для того, чтобы рассмотреть еще один механизм следообразования и, соответственно, форму, обозначив ее как невербально-информационную.

Представим, что для определения правдивых или ложных показаний подозреваемого, свидетеля, обвиняемого используется получение информации путем фиксации их невербального поведения, как визуально, так и с помощью технических средств, в том числе средствами видеозаписи.

Известно, что невербальное поведение – это способность человека выражать свои мысли мимикой, движениями глаз, губ, рук, других частей тела, которые выступают в качестве информативных проявлений его сущности.

Доказано, что как только человек начинает лгать (обманывать, говорить неправду, вводить в заблуждение и т. д.), его тело самопроизвольно совершает некоторые движения, по которым он может быть уличен во лжи. Это связано с тем, что в процессе так называемого обмана подсознание посылает некие нервные импульсы, которые проявляют себя в виде жестов, противоречащих тому, что сказал человек. Именно мимика, жесты, движения являются одной из первых визуальных знаковых систем. Ученые выявили и зарегистрировали более тысячи невербальных знаков и сигналов. Лишь 7 % информации в беседе передается непосредственно словами, звуками и интонацией – до 38 %, а жестами, позой и телодвижениями – до 55 %.

Учитывая это обстоятельство, мы рассмотрим невербальное поведение человека (A_1) за счет преобразования визуальных знаковых систем (*Z*) в информационные коды (*K*) как механизм невербально-информационного следообразования (*NI*) между изучаемым и изучающим экспертом (B_2). Такое образование можно выразить следующим образом:

$$(Os_1)\ A_1 = I(Zc) - (K) - NI = (B_2\ Osv_2).$$

Учитывая классическую схему, представим, что следообразующим объектом (Os_1) исследования является человек с признаками невербального поведения (A_1), от которого в результате наблюдения мы получаем информацию (*I*) в виде знаковых систем (*Zc*) (невербальные движения), используем кодовое

преобразование (K), которое выражается в виде следового контакта, то есть механизма невербально-информационного следообразования (NI), которое сможет исследовать эксперт (B_2) как объект следовоспринимающий (Osv_2) и вынести заключение (Y) о правдивых или ложных показаниях. Представим это предположение в виде формулы

$$A_1(Os_1) = I - Z - (K) - NI - B_2(Osv_2) = Y.$$

Таким образом, мы наглядно продемонстрировали, что виртуально-информационные следообразования представляют собой универсальный механизм изменения состояний объектов в результате кодовых преобразований – от следообразующего до следовоспринимающего объекта и следового контакта.

Благодаря своей универсальности приведенные выше следообразования можно определять и идентифицировать в информационном, виртуальном пространстве с точки зрения криминалистики, компьютерных, видеозаписывающих и иных цифровых устройствах, их системах и сетях, определяя механизм воздействия от начального к конечному и обратно.

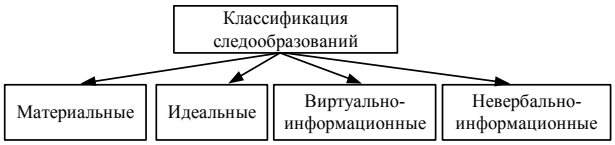
Такая форма не подпадает под классификацию [14] механизма и характера следообразований, таких как следы-отражения, следы-вещества и следы-предметы, что говорит о необходимости ее выделения в отдельную группу.

Стоит учитывать и тот факт, что на сегодняшний день возникла объективная необходимость в процессуальных процедурах по фиксации и исследованию виртуальных источников информации в качестве самостоятельных источников доказательств [15], определяя, соответственно, набор терминов, определений и классификацию следообразований, где представляемая форма будет весьма полезной, поскольку в Уголовно-процессуальном кодексе Российской Федерации они полностью отсутствуют.

Что касается невербально-информационного следообразования, то оно тоже является сугубо индивидуальным и не подпадает под классическую форму следообразований, но подлежит идентификации (хотя в том числе и с помощью видеоаппаратуры), что дает полное право на существование.

Данная форма уже взята на вооружение при расследовании уголовных дел и экспертных исследований, хотя пока и не является доказательством по делу, но тем не менее можно с полной уверенностью говорить о включении данной формы в общую классификацию криминалистических следообразований.

Таким образом, классификацию основных криминалистических следообразований можно представить в виде следующей схемы:



Именно такой предполагаемый порядок основных (базовых) следообразований позволит своевременно проводить идентификацию следов и криминалистически грамотно их классифицировать в дальнейшем.

Библиографические ссылки

1. Криминалистика : курс лекций для бакалавров / под ред. М. К. Каминского, А. М. Каминского. – Ижевск : Jus est, 2012. – 358 с.

2. *Григоренко С. В.*, *Ткаченко С. Н.*, *Каспаров А. А.* Преступления в сфере компьютерной информации. – М. : ПОЛТЕКС, 2003. – 40 с.

3. Проблемы уголовно-процессуальной науки XXI // Сб. ст. Междунар. науч.-практ. конф., посвящ. 75-летию д-ра юр. наук, проф. З. З. Зинатуллина. – Ижевск, 2013. – 557 с.

4. *Камалова Г. Г.* Криминалистическая методика расследования преступлений в сфере информационных технологий // Криминалистика : курс лекций для бакалавров / под ред. М. К. Каминского, А. М. Каминского. – Ижевск : Jus est, 2012. – 358 с.

5. *Мещеряков В. А.* Преступления в сфере компьютерной информации : Основы теории и практики расследования. – Воронеж : Изд-во Воронеж. гос. ун-та, 2002. – С. 94–119.

6. *Волеводз А. Г.* Противодействие компьютерным преступлениям. – М., 2002. – С. 159–160.

7. *Семенов А. Ю.* Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. – 2004. – № 1.

8. *Краснова Л. Б.* Компьютерные объекты в уголовном процессе и криминалистике : автореф. дис. … канд. юр. наук. – Воронеж, 2005. – С. 17.

9. *Черкасов В. Н.*, *Нехорошев А. Б.* Кто живет в «киберпространстве»? // Управление защитой информации. – 2003. – Т. 7. – № 4. – С. 468.

10. *Милашев В. А.* Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. … канд. юр. наук. – М., 2004. – С. 18.

11. *Лыткин Н. Н.* Использование компьютерно-технических следов в расследовании преступлений против собственности : автореф. дис. … канд. юр. наук. – М., 2007. – С. 11.

12. Там же. – С. 12.

13. *Каминский М. К.* Цифровые технологии в криминалистике и судебной экспертизе : курс лекций. – Ижевск : Jus est, 2012. – С. 46–47.

14. *Белкин Р. С.* Курс криминалистики : в 3 т. – Т. 2 : Частные криминалистические теории. – М. : Юристь, 1997. – С. 53–55.

15. Проблемы уголовно-процессуальной науки XXI // Сб. ст. Междунар. науч.-практ. конф., посвящ. 75-летию д-ра юр. наук, проф. З. З. Зинатуллина. – Ижевск, 2013. – 457 с.

P. V. Mochagin, PhD in Law, Associate Professor, Udmurt State University, Izhevsk

Identification of Virtual Information and Nonverbal Marking Formation As the New Direction in Criminalistics

The concept and essence of virtual information and nonverbal mechanisms of marking formation and its role in crime investigation are revealed.

Key words: criminalistics, computer crimes, digital information, polygraph, virtual information and nonverbal information mechanisms of marking formation.