5. Стрэнг Р. *Практика страхования профессиональной ответственности адвокатов в США*. Вестник адвокатской палаты Иркутской области №10, 2006.

6. Научно-практический комментарий к Федеральному закону от 31 мая 2002 г. N 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (под общ. ред. докт. юрид. наук., проф. А.Г. Кучерены). М.: «Деловой двор», 2009.

7. Кратенко М. *Страхование профессиональной ответственности адвоката*. В: Право и экономика, № 10 от 30.10.2004.

8. Скуратов А. Н. *Страховка для адвоката*? В: Воронежский адвокат, №5, 2009.

9. Никифоров И., Рогожин С. *Страхование профессиональной деятельности адвокатов в Европейском Союзе и Германии*. В: Адвокат (газета) 2004, №8(157).

10. Rudiger Boergen. *Die vertrauliche Haftung des Rechtsanwalts.* Berlin, 1968.

11. Кратенко М. В. *Страхование профессиональной ответственности адвоката*. В: Право и экономика, 2004, N 10.

12. Наумов Д. В. Автореф. дис.: *Гражданско-правовое регулирование обязательного страхования профессиональной имущественной ответственности адвокатов.* [ВолГУ]. Волгоград, 2011, на электронном ресурсе http://lib.volsu.ru/. Дата обращения 01.10.13.

13. Закон Французской Республики № 71-1130 от 31 декабря 1971 г. *об организации адвокатской профессии* и Декрет, утвержденного Указом № 91-1197 от 27 ноября 1991 г., на электронном ресурсе www.legifrance.gouv.fr. Дата обращения 02.10.13.

14. Итальянский Королевский Декрет-Закон № 1578/1933 и Закон № 247 от 31 декабря 2012 г. *об адвокатуре и адвокатской деятельности*, на электронном ресурсе www.studiolegalegrasso.net/ru. Дата обращения 03.10.13.

15. Legea nr. 51/1995 pentru organizarea şi exercitarea profesiei de avocat, republicată în Monitorul Oficial al României, Partea I, nr.113 din 6 martie 2001. Statutul profesiei de avocat. Textul actului publicat în M.Of. nr. 284/31 mai 2001, на электронном ресурсе www.avocatul.ro. Дата обращения 02.10.13.

16. Федеральный Закон Российской Федерации *«Об адвокатской деятельности и адвокатуре в РФ»*, на электронном ресурсе Ошибка! Недопустимый объект гиперссылки. обращения 05.10.13

17. Кратенко М. В., Шевцова И. Г. *Перспективы страхования профессиональной ответственности адвоката в России*. В: Услуги: проблемы правового регулирования и судебной практики: сб. науч.-практ. ст. М., Волтерс Клувер, 2007.

ОСОБЕННОСТИ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И СОТОВОЙ СВЯЗИ

О. МУСИЕНКО,
кандидат юридических наук, доцент кафедры криминалистики Национального юридического университете им. Ярослава Мудрого (Украина)

SUMMARY

The paper discusses various approaches to understanding the forensic characteristics of the crimes committed in the area of computer information and mobile communication. The analysis of the elements of criminal characteristic and installed their features.

Keywords: forensic characterization, computer information, cellular communications, computer, internet, hacker, server, virtual tracks.

***

В работе рассматриваются различные подходы к пониманию криминалистической характеристики преступлений, совершаемых в сфере компьютерной информации и сотовой связи. Проведен анализ элементов криминалистической характеристики и установлены их особенности.

Ключевые слова: криминалистическая характеристика, компьютерная информация, сотовая связь, компьютер, интернет, хакер, сервер, виртуальные следы.

Постановка проблемы. С развитием компьютерных технологий и средств сотовой связи появились новые виды преступлений, объектом преступного посягательства которых являются информация и права на нее, безопасность пользования средствами сотовой связи. Возникает острая необходимость правовой защиты такого рода информации от преступного посягательства, что послужило поводом для разработки новых средств по выявлению, расследованию и предупреждению преступлений, совершаемых с использованием компьютерной техники и средств сотовой связи.

Актуальность темы. Проблемам криминалистической характеристики посвятили работы многие ученые – криминалисты: Р.С. Белкин, И.А. Возгрин, И.Ф. Герасимов, А.Н. Васильев, Л.Я. Драпкин, В.Ф. Ермолович, А.Н. Колесниченко, В.А. Образцов, Л.Д. Самыгин, В.Г. Танасевич, Н.П. Яблоков и др.

Вместе с тем, отмечая значительный вклад этих и других ученых, которые изучали отдельные аспекты криминалистической характеристики конкретных видов преступлений, данная проблема далеко не исчерпана и требует дальнейших научных исследований. В настоящее время среди авторов нет единого мнения, какие элементы необходимо включать в содержание криминалистической характеристики преступлений, которые совершаются в сфере компьютерной информации и сотовой связи. Отсутствует единый подход к определению понятия «компьютерная информация». Именно проблемам криминалистической характеристики данного вида преступлений, как одного из элементов методики расследования преступлений, посвящена эта статья, в чем и

заключается ее актуальность и новизна.

Цель статьи – выявление особенностей криминалистической характеристики преступлений, которые совершаются в сфере компьютерной информации и сотовой связи, а также установить особенности компьютерной информации и информации, которая сосредоточена в средствах сотовой связи.

Изложение основного материала исследования. Криминалистическая характеристика имеет большое значение в методике расследования преступлений. Проблемам криминалистической характеристике посвящено много работ, однако до сих пор не существует единого определения криминалистической характеристики. Так, Н.П. Яблоков, Л.Д. Самыгин считают, что криминалистическая характеристика – это система описания криминалистически значимых признаков вида, группы и отдельного преступления, проявляющихся в особенностях способа, механизма и обстановки его совершения, дающая представление о преступлении, личности его субъекта и иных обстоятельствах, об определенной преступной деятельности и имеющая своим назначением обеспечение успешного решения задач раскрытия, расследования и предупреждения преступлений [1, с. 34].

И.Ф. Герасимов определяет криминалистическую характеристику как совокупность сведений, знаний об отдельном виде или группе преступлений, полученных в результате специальных исследований, являющуюся важным структурным элементом методики расследования, обусловливающую методические рекомендации и в конечном счете способствующую раскрытию, расследованию и предупреждению преступлений [2, с. 7].

Как справедливо отмечает В.Ф. Ермолович, криминалистическая характеристика – это система криминалистически значимой информации о преступлении, разрабатываемая и используемая для повышения эффективности выявления, раскрытия, расследования и предупреждения преступлений [3, с. 278]. Как видно из этих определений, именно криминалистическая характеристика позволяет разработать и эффективно использовать методику расследования любого преступления, в том числе и в сфере компьютерной информации и сотовой связи.

Проблеме криминалистической характеристики преступлений в сфере компьютерной информации посвящен ряд работ, при этом у различных авторов ее понятие незначительно отличается. Е.Н. Быстряков, А.Н. Иванов, В.А. Климов понимают под криминалистической характеристикой систему обобщенных данных о типичных элементах компьютерных преступлений и закономерных связях между ними, значимых для решения задач, стоящих перед органами следствия и дознания [4, с. 7]. Ю В. Гаврилин определяет криминалистическую характеристику преступлений в сфере компьютерной информации как систему обобщенных данных о типичных следах, способе совершения и механизме преступления, личности преступника и других существенных чертах, свойствах и особенностях преступления и сопутствующих ему обстоятельствах, способствующую оптимизации расследования и практическому применению средств, приемов и методов криминалистики в раскрытии и расследовании данного преступления [5, с. 56].

Анализируя данные определения, можно сделать вывод, что криминалистическая характеристика преступлений в сфере компьютерной информации и сотовой связи – это система информации о криминалистически значимых, взаимосвязанных признаках этого преступления, служащую целям наиболее эффективного выявления, раскрытия, расследования и предупреждения этих преступлений.

Криминалистическая характеристика является одним из важных и основных теоретических и практических источников получения криминалистически значимой информации о различных видах преступлений [6, с. 26]. В качестве обобщающего понятия информации в ее познавательной сущности в криминалистике выделена криминалистически значимая информация, представляющая собой информацию, могущую выступать в качестве доказательств по уголовному делу или способствующая получению таковой, а также любая иная информация, имеющая значение для достижения установленных законом конечных целей деятельности по раскрытию и расследованию преступлений [7, с. 237]. С точки зрения процесса расследования преступлений важно отметить, что информация, в том числе и криминалистически значимая, обладает рядом свойств, ее можно: создавать, передавать, хранить и обрабатывать. Так, событие преступления сопровождается созданием информации – формируется следовая картина, участники расследования ее воспринимают, передают друг другу, определенным образом сохраняют и интерпретируют.

Поскольку криминалистически значимая информация обращается в сфере раскрытия, расследования и предупреждения преступлений криминалистическими средствами [8, с. 22], в криминалистике появилось такое понятие, как информационные системы криминалистического

содержания. По мнению В.А. Козинкина, средства сотовой связи являются целостной информационной системой, выступающей в качестве потенциального источника криминалистически значимой информации [9, с. 13]. Сущность информационных свойств средств сотовой связи как источника получения информации, в том числе и криминалистически значимой, вытекает из анализа понятий «средства связи», «сеть связи», принципов построения и функционирования вышеуказанных сетей.

Характеризуя информацию, обнаруживаемую в средствах сотовой связи, следует отметить, что она может носить характер как потенциально, так и актуально криминалистически значимой информации. Так любая информация, возникающая в ходе эксплуатации пользовательского оборудования непосредственно в нем самом и в операционно-информационных системах и центрах коммутации оператора сотовой связи, выступает в качестве потенциальной, а характер актуальной она приобретает тогда, когда устанавливается ее прямая причинно-следственная связь с событием преступления. При этом, формой существования этой информации является информационный объект – файл, который обладает фиксированной структурой и определенными параметрами, поддерживаемыми операционной системой.

Таким образом, знание криминалистической характеристики позволяет определить направление и средства расследования, а также выдвинуть обоснованные версии о произошедшем, установить отсутствующие факты. В систему элементов криминалистической характеристики практически все юристы включают сведения о мотивах и целях преступления, способах совершения и сокрытия преступления, личности преступника, личности потерпевшего и предмете посягательства, взаимосвязи с другими преступлениями, типичных обстоятельствах совершения преступления [10, с. 8]. Следует заметить, что большое значение имеет не только наличие тех или иных элементов, но и существующие между ними взаимосвязи.

При расследовании преступлений в сфере компьютерной информации и сотовой связи предметом посягательства является компьютерная информация. В настоящее время нет единого мнения, что необходимо понимать под компьютерной информацией. Первым понятие компьютерной информации сформулировал И.З. Карась, который определил ее как информацию, которая циркулирует в вычислительной среде, зафиксированную на физическом носителе в форме, доступной для понимания ЭВМ, или передается телекоммуникационными каналами [11, с. 40]. С криминалистической точки зрения это понятие исследовал В.В. Крылов и пришел к выводу, что как предмет преступного посягательства компьютерная информация – это сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею [12, с. 35].

Е.Р. Россинская считает, что компьютерная информация в процессе доказывания – это фактические данные, обработанные компьютерной системой, и (или) те, которые передаются по телекоммуникационным каналам, доступные для восприятия, и на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного или гражданского дела [13, с. 30].

В Уголовном кодексе Украины компьютерная информация определяется, как текстовая, графическая или любая другая информация (данные), которая существует в электронном виде, сохраняется на соответствующих носителях и которые можно создавать, изменять или использовать при помощи ЭВМ [14].

В криминалистической характеристике преступлений важное значение имеет обстановка совершения преступления. Элементы обстановки совершения преступления оставляют различного рода следы вовне, которые могут быть выявлены и изучены при расследовании. Обстановка совершения преступления в сфере компьютерной информации и сотовой связи имеет свою специфику. Такие преступления совершаются в определенной среде – в сфере деятельности ЭВМ. Особенностью подобных преступлений является то, что на них не влияют природно-климатические факторы [15, с. 113], то есть они могут совершаться в любом месте, где функционирует ЭВМ.

Особенность совершения деяния и сложность данного преступления состоит в том, что общественно опасное деяние может совершаться на территории одного государства, а последствия наступают на территории другого. К тому же с учетом устройства сети Интернет следы преступления могут находиться на сервере провайдера, который физически находится на территории третьей страны. На успех раскрытия таких преступлений большое влияние оказывает степень взаимного сотрудничества государств.

Немаловажным моментом также является неидентичность законодательства разных стран в области борьбы с преступлениями в сфере высоких технологий и Интернета. Европейский союз уже достаточно давно разрабатывает различные методы

сотрудничества и общие законы для стран-участниц, так как Интернет есть во всех странах и многие преступления совершаются иностранными гражданами, находящимися в иных государствах, где ответственность за такие преступления не предусмотрена.

В нашей стране подписано соглашение «О сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации». В соответствии с этим соглашением стороны будут сотрудничать в обеспечении предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации.

Преступления, совершаемые в сфере компьютерных технологий и сотовой связи – преступления в сфере высоких технологий. Следовательно, этим в первую очередь определяется характеристика личности человека, совершающего данное преступление. Совершить подобное преступление под силу далеко не каждому человеку, несмотря на массовую компьютеризацию страны.

Криминалистические сведения о личности подозреваемого в преступлении человека включают в себя сведения о социальном статусе личности, о социальной функции в обществе, о нравственно-психологической характеристике, а также особенностях поведения во время совершения преступления. Проблемам личности преступника, совершающего преступления в сфере компьютерной информации, посвятили свои работы многие криминалисты. В настоящее время в литературе, каклибо связанной с компьютерами, часто встречается иностранное слово «хакер», трактующееся в разных работах по-разному. Профессия лиц, совершающих данное преступление, как правило, связана с использованием или настройкой компьютеров и программного обеспечения к ним. По мнению В. Г. Проскурина, хакер, осуществляющий неправомерный доступ к компьютерной информации, может выступать в одной из следующих ролей: постороннее лицо, использующее глобальную сеть; сотрудник организации, не имеющей легального доступа к системе; пользователь, обладающий минимальными полномочиями; администратор системы; разработчик системы [16].

Увлечение лиц, совершающих данные преступления, связаны с ПК. Они проводят много времени за компьютером, работая с программным обеспечением, модифицируя и изменяя его, создают новые утилиты, часто бывают в сети Интернет. Н. Н. Ахтырская предлагает дополнить психологический портрет преступника исследованием характеристики ума, индивидуальность которого проявляется в широте, глубине, самостоятельности, критичности, быстроте и гибкости [17, с. 99]. Компьютерные преступники – это уже вполне сформировавшиеся личности, обладающие высокими профессиональными и устойчивыми преступными навыками, а также определенным жизненным опытом. Совершаемые ими деяния носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления. Преступления, которые носят серийный, многоэпизодный характер, обязательно сопровождаются действиями по сокрытию. Это обычно высококвалифицированные специалисты с высшим математическим, инженерно-техническим или экономическим образованием, входящие в организованные преступные группы и сообщества, прекрасно оснащенные технически (нередко специальной оперативной техникой). Особую опасность с точки зрения совершения преступлений в сфере компьютерной информации представляют профессионалы в области новых информационных технологий. На долю этой группы приходится большинство особо опасных должностных преступлений, совершаемых с использованием средств компьютерной техники, присвоений денежных средств в особо крупных размерах, мошенничества и проч.

Информация об особенностях личности потерпевшего позволяет выяснить ряд вопросов, касающихся различных обстоятельств совершения преступления. В современной литературе высказывается мнение, что потерпевшим от преступления в сфере компьютерной информации чаще всего является юридическое лицо [18, с. 33]. Однако с каждым годом количество людей, использующих ЭВМ в частной жизни, увеличивается и доступ в сеть. Интернет в настоящее время общедоступен. Изучение уголовных дел показывает, что наиболее часто потерпевшими от преступлений в сфере компьютерной информации являются кредитно-финансовые учреждения (72%), частные лица (14%), интернет-провайдеры (5%) , общественные организации и государственные учреждения (8%).

Немаловажное значение в криминалистической характеристике преступления имеет мотив. При расследовании мотив преступления может указать направление поиска, и в связи с этим его выяснение необходимо для раскрытия преступления. Мотивы преступлений в сфере компьютерной информации изучаются многими авторами. Так, В.Б. Вехов [19, с. 41], В.А. Мазуров [20, с. 117] выделяют следующие виды мотивов: 1) ко-

рыстные соображения; 2) политические мотивы; 3) исследовательский интерес; 4) хулиганские побуждения и озорство; 5) месть. Е. Н. Быстряков, А. Н. Иванов и В. А. Климов предлагают дополнительно выделить следующий мотив: дезорганизация работы учреждения, предприятия или системы с целью устранения конкурента, стремления скрыть другое преступление [4, с. 33].

В.А. Мещеряков выделяет иные приоритетные мотивы: 1) месть; 2) достижение материальной выгоды, в том числе за счет продажи полученной информации; 3) хулиганство и любопытство; 4) профессиональное самоутверждение [21, с. 110].

Важнейшим и определяющим элементом криминалистической характеристики любого преступления является способ его совершения. Анализ конкретных преступлений, совершенных с использованием компьютерной техники, позволяет выделить несколько десятков способов их совершения, которые постоянно совершенствуются и модифицируются. Подобное многообразие обусловлено как сложностью аппаратного и программного обеспечения ЭВМ, так и многообразием осуществляемых информационных операций, связанных с движением материальных ценностей, финансовых и денежных средств, научно-технических разработок, «ноу-хау» и т. д.

На сегодняшний день в криминалистике нет единой классификации способов совершения преступлений в сфере компьютерной информации. Одна из классификаций предложена А. Н. Родионовым и А. В. Кузнецовым. Согласно ей, способы совершения компьютерных преступлений можно подразделить: 1) на «изъятие средств компьютерной техники; 2) неправомерный доступ к компьютерной информации: преступления, совершенные в отношении компьютерной информации, находящейся в глобальных компьютерных сетях; преступления, совершенные в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.); 3) изготовление или распространение вредоносных программ (вирусы, программы – взломщики и т.п.); 4) перехват информации: электромагнитный; непосредственный; 5) нарушение авторских прав (компьютерное пиратство); 6) комплексные методы [22, с. 37].

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран. Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q . Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного: **QA** - несанкционированный доступ и перехват; QAH – компьютерный абордаж; QAI – перехват; QAT - кража времени; QAZ - прочие виды несанкционированного доступа и перехвата; **QD** - изменение компьютерных даннях; QUL - логическая бомба; QDT - троянский конь; QDV - компьютерный вирус; QDW - компьютерный черв; QDZ - прочие виды изменения данных; **QF** - компьютерное мошенничество; QFC - мошенничество с банкоматами; QFF - компьютерная подделка; QFG - мошенничество с игровыми автоматами; QFM - манипуляции с программами ввода-вывода; QFP - мошенничества с платежными средствами; QFT - телефонное мошенничество; QFZ - прочие компьютерные мошенничества; **QR** - незаконное копирование ; QRG - компьютерные игры; QRS - прочее программное обеспечение; QRT - топография полупроводниковых изделий; QRZ - прочее незаконное копирование; **QS** - компьютерный саботаж ; QSH - с аппаратным обеспечением; QSS - с программным обеспечением; QSZ - прочие виды саботажа; **QZ** - прочие компьютерные преступления ; QZB - с использованием компьютерных досок об'явлений; QZE - хищение информации, составляющей коммерческую тайну; QZS - передача информации конфиденциального характера; QZZ - прочие компьютерные преступления [23].

В расследовании преступлений важное место занимают следы. Следы преступления применяются для обозначения всех самых разнообразных материальных изменений, которые обязаны своим происхождением тем или иным действиям преступника. Говоря о следах в сфере компьютерной информации, интересным представляется мнение В.А. Мещерякова, который выделяет следы в сфере компьютерной информации в отдельную группу так называемых «виртуальных следов», что обусловлено специфическими свойствами, присущими только таким следам. По его мнению, виртуальный след – это любое криминалистически значимое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации на материальном носителе, в том числе на электромагнитном поле [21, с. 73].

Некоторые авторы не согласны с выделением следов в сфере компьютерной информации в отдельную группу виртуальных следов, так как они считают, что в такой группе следов, как и в любой другой, существуют воздействующие объекты, объекты, передающие воздействие, воспринимающие объекты. И все эти предметы, процессы, следы могут быть только материальными и никакими иными, и даже идеальные следы, находящиеся в памяти, материальны, поскольку уничтожение мозга повлечет уничтожение таких следов [24, с. 129].

Следы средств компьютерной техники – очень широкое понятие, и вследствие этого не представляется возможным отнести их к одной группе следов (материальных, идеальных или виртуальных). Следы средств компьютерной техники бывают весьма разнообразны: распечатка текста, графического рисунка или схемы, компакт-диск с информацией, виртуальный образ, информация в радиоволне, в инфракрасном луче, мысленный образ изображения, увиденного очевидцем на дисплее ЭВМ, и пр.

Таким образом, следы средств компьютерной техники – это любые изменения среды, обусловленные работой таких средств и возникшие в результате совершения в этой среде преступления.

Выводы. Проведенное нами исследование позволяет сделать вывод о том, что криминалистическая характеристика преступлений, которые совершаются в сфере компьютерной информации и сотовой связи, содержит такие элементы, как: способ совершения, предмет посягательства, обстановку совершения преступления, личность преступника и личность жертвы, а также следы. При этом, поскольку данный вид преступления совершается в сфере высоких технологий, то и перечисленные элементы имеют свою специфику, которая характерна для преступлений, которые совершаются в сфере компьютерной информации и сотовой связи.

Литература

1. Яблоков Н. П., Самыгин Л. Д. *Информационные основы расследования и криминалистическая характеристика преступлений*. В: Криминалистика. М.: БЕК, 1995, с. 44.

2. Герасимов И. Ф., Цыпленкова Е. В. *Общие положение методики расследования преступлений*. В: Криминалистика. М.: Высшая школа, 1994, с. 333.

3. Ермолович В. Ф. *Криминалистическая характеристика преступлений*. Минск: Амалфея, 2001..

4. Быстряков Е. Н., Иванов А. Н., Климов В. А. *Расследование компьютерных преступлений*. Учеб.пособие. Под ред. В. И. Комиссарова. Саратов: СГАП, 2000.

5. *Преступления в сфере компьютерной информации: квалификация и доказывание*. Учеб. Пособие. Под ред. Ю. В. Гаврилина. М.: ЮИ МВД России, 2003.

6. Яблоков Н. П. *Криминалистическая характеристика преступлений – важный элемент криминалистической теории и практики*. В: Актуальные проблемы криминалистики на современном этапе. Материалы Всероссийской научно-практической конференции (г. Краснодар, 23-24 мая 2002 г.). Краснодар, 2002.

7. Белкин Р. С. *Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики*. М.: Норма, 2001.

8. Салтевский М. В. *Собирание криминалистической информации техническими средствами на предварительном следствии*. Учебное пособие. Киев, 1980.

9. Козинкин В. А. *Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи*. Монография. М.: Изд-во Юрлитинформ, 2010.

10. Менжега М. М. *Методика расследования создания и использования вредоносных программ для ЭВМ*. М.: Юрлитинформ, 2010.

11. Карась И. З. *Экономический и правовой режим информационных ресурсов*. В: Право и информатика. Под ред. Е. А. Суханова. М.: Изд-во МГУ, 1990.

12. Крылов В. В. *Информационные компьютерные преступления*. М.: НОРМА-ИНФРА-М, 1997.

13. Россинская Е. Р., Усов А. И. *Судебная компьютерно-техническая экспертиза.* М.: Право и Закон, 2001.

14. Кримінальний кодекс України. В: Відомості Верховної Ради України (ВВР), 2001, №25-26, ст..131.

15. Шурухнов Н. Г. *Расследование неправомерного доступа к компьютерной информации*. М.: Щит-М, 1999.

16. Проскурин В. Г. *Автоматизированная банковская система глазами хакера*. [электронный ресурс]. Центр исследования проблем компьютерной преступности. http://www.crime-research.ru.

17. Ахтырская Н. Н. *Проблемы ювенальной психологии лиц, совершающих преступления в сфере информационных технологий*. В: Современное состояние и перспективы развития новых направлений судебных экспертиз в России и за рубежом. Материалы междунар. науч.- практ. конференции. Калининград, 23-24 апреля 2003 г., с. 98-99.

18. Быстряков Е. Н., Иванов А. Н., Климов В. А. *Расследование компьютерных преступлений*. Саратов: СГАП, 2000.

19. Вехов В. Б. *Компьютерные преступления: Способы совершения и раскрытия*. Под ред. акад. Б. П. Смагоринского. М.: Право и закон, 1996.

20. Мазуров В. А. *Компьютерные преступления: классификация и способы противодействия*. Учеб.-практ. пособие. М.: Палеотип, Логос, 2002.

21. Мещеряков В. А. *Преступления в сфере компьютерной информации: правовой и криминалистический анализ*. Воронеж, 2001.

22. Родионов А. Н., Кузнецов А. В. *Расследование преступлений в области высоких технологий*. Вестник МВД России, 1999, № 6.

23. *Классификация компьютерных преступлений по кодификатору Генерального Секретариата Интерпола* [Электрон. ресурс]. Доступно из URL: http://www.cyberpol.ru/cybercrime.shtml.

24. Черкасов В. Н., Нехорошев А. Б. «Виртуальные следы» в «кибернетическом пространстве». В: Судебная экспертиза: Межвуз. сб. науч. ст. Вып. 2-й. Саратов: СЮИ МВД России, 2003, с. 127-130.