На правах рукописи

Коломинов Вячеслав Валентинович

РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: НАУЧНО-ТЕОРЕТИЧЕСКАЯ ОСНОВА И ПРИКЛАДНЫЕ АСПЕКТЫ ПЕРВОНАЧАЛЬНОГО ЭТАПА

12.00.12 – Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2017

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Байкальский государственный университет» (г. Иркутск)

Научный руководитель – **Степаненко Диана Аркадьевна**
доктор юридических наук, профессор

Официальные оппоненты: **Мещеряков Владимир Алексеевич**
доктор юридических наук, профессор
ФГБОУ ВО «Воронежский государственный университет», профессор кафедры криминалистики

Шурухнов Николай Григорьевич
доктор юридических наук, профессор
Тульский институт (филиал) ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)», профессор кафедры уголовно-правовых дисциплин

Ведущая организация – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Балтийский федеральный университет им. Иммануила Канта»

Защита диссертации состоится « 12 » мая 2017 г. в $12^{\underline{00}}$ часов на заседании диссертационного совета Д 220.038.11 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», по адресу: 350044, г. Краснодар, ул. Калинина, 13, главный учебный корпус университета ауд. 215.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина» и на сайте www.kubsau.ru.

Автореферат разослан «___» _____ 2017 г.

Ученый секретарь
диссертационного совета Шульга Андрей Владимирович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Все больше информации в настоящее время хранится и обрабатывается в компьютерных системах. Использование компьютерно-технических средств для обработки и обмена информацией между различными частными и государственными структурами практически во всех отраслях жизни общества является, позитивным моментом, отвечающим требованиям времени. С одной стороны, это в значительной степени позволяет ускорить социально-экономические процессы, происходящие в современном обществе и увеличить скорость информационного обмена. С другой стороны, появилась киберпреступность. Так, экономике России действиями киберпреступников разного уровня нанесён ущерб в 203,3 млрд. руб., что равно 0,25% объёма ВВП, в 2015 году прямой финансовый ущерб составил 123,5 млрд. (0,15% от ВВП), а затраты на ликвидацию последствий более 79,8 млрд. (0,1% от ВВП). Такие сведения опубликованы в совместном исследовании Group-IB, Фонд развития Интернет-Инициатив (ФРИИ) и Microsoft. В течение четырех кварталов – со II квартала 2015 года по I квартал 2016 года киберпреступники украли около 5,5 млрд. руб., что на 44% больше похищенного за предыдущий отчетный период, сделала вывод Group-IB в исследовании[1].

В России пока недостаточно опыта и сил, чтобы противостоять киберпреступности, ущерб от которой растет, заявил премьер-министр России Д.А. Медведев на совещании по вопросу «об информационной безопасности в кредитно-финансовой сфере России»[2].

На сегодняшний день в различных государственных и негосударственных учреждениях на электронных носителях, содержится колоссальный объем различной информации, в том числе о конкретных лицах, осуществляемой деятельности, месте регистрации и жительства, перемещении в пространстве, осуществляемых сделках, банковских и иных финансовых операциях, наличии движимого и недвижимого имущества и прочее. Это далеко не полный перечень, составляющий такую информацию. На первый взгляд, развитие электронных баз данных и компьютеризация человеческой деятельности должны только положительно влиять на процессы развития общества в целом. Для криминальных лиц обладание информацией любого свойства открывает огромные возможности использования ее в конкретных корыстных преступных целях. Тем более, что использование компьютерно-технических средств и иных технически сложных устройств с подключением к компьютерным сетям позволяет злоумышленнику совершать преступления, находясь на значительном расстоянии от своей жертвы, а это в значительной степени затрудняет выявление и расследование таких противоправных деяний, обусловли-

[1] [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Россия (дата обращения: 17.10.2016).

[2] [Электронный ресурс]. URL: http://vz.ru/news/2016/6/3/814274.html (дата обращения: 17.10.2016).

вая высокий уровень их латентности. Ущерб от криминальной деятельности лиц, совершающих преступления в сфере компьютерной информации колоссальный. Это в полной мере относится к таким преступлениям, как мошенничество.

Разрабатывая различные схемы и способы совершения мошенничества в сфере компьютерной информации, получившего широкое распространение, преступники активно используют достижения научно-технического прогресса в области высоких компьютерных технологий, применяя знания в области компьютерной техники и программирования. Движимые корыстными мотивами, криминальные субъекты объединяются в устойчивые преступные группы, носящих зачастую, транснациональный характер. При этом жертвами преступных деяний становятся не только конкретные физические лица, но и юридические лица всех форм собственности, а также публично-правовые образования (государственные и муниципальные органы, учреждения и организации).

Перед государством возникла необходимость принятия соответствующих адекватных мер, позволяющих эффективно противодействовать фактам мошенничества, совершаемого в сфере компьютерной информации. Президент РФ В. Путин в ходе выступления на расширенном заседании коллегии Федеральной службы безопасности Российской Федерации (26 февраля 2016 года) поручил ведомству разработать систему защиты от информационных угроз и киберзлоумышленников[3].

Федеральным законом от 29.11.2012 г. №207-ФЗ мошенничество в сфере компьютерной информации законодателем было выделено в самостоятельную норму. Включенная в Уголовный кодекс Российской Федерации статья 159^6 стала предусматривать ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей.

Следует признать, что борьба с проявлениями мошенничества в сфере компьютерной информации будет эффективной только тогда, когда правоохранительные органы будут вооружены научными положениями и разработанными на их основе практическими рекомендациями по расследованию данного вида преступлений. В настоящее время следователи и оперативные работники пока продолжают пользоваться рекомендациями по расследованию компьютерных преступлений, которые при кажущейся схожести, имеют другую специфику. Это, безусловно, сказывается на снижении способности правоохранительных органов своевременно выявлять и раскрывать факты совершенного мошенничества в сфере компьютерной информации. Как свидетельствует анализ следственной и судебной практики, органы предварительного расследования испытывают определенные трудности, связанные с расследованием преступлений, предусмотренных 159^6 УК РФ, и пре-

[3] [Электронный ресурс]. URL: http://portaltele.com.ua/news/officially/2013-02-14-13-34-52.html (дата обращения: 17.10.2016).

сечением преступной деятельности мошенников. Отчасти это связано и с недостаточной профессиональной подготовкой лиц, осуществляющих выявление и расследование данного вида мошенничества.

Нельзя полагать, что ранее мошенничество в сфере компьютерной информации не совершалось, и не было объектом научного изучения. Опыт борьбы правоохранительных органов с данным видом преступлений, теоретические разработки прошлых лет, нормативно-правовая база послужили основой для настоящего исследования и позволили на основе комплексного, системного подхода сформулировать научные положения и осуществить разработку криминалистических рекомендаций по расследованию мошенничества в сфере компьютерной информации, в частности его первоначального этапа.

Актуальность диссертационного исследования обусловлена, с одной стороны, высокой практической значимостью, а с другой – недостаточной разработанностью некоторых вопросов методики расследования мошенничества в сфере компьютерной информации.

Степень разработанности темы исследования. Мошенничество – традиционное, достаточно изученное в уголовно-правовой, уголовно-процессуальной, криминалистической науке, но способ и механизм этого преступления нов и специфичен. Поэтому, как объект научного познания, мошенничество в сфере компьютерных преступлений требует интегрального комплексного подхода с обязательным привлечением достижений таких наук, как кибернетики, информатики, экономики, криминалистики, уголовного права, уголовного процесса, общей теории судебных экспертиз.

Вопросам мошенничества в различных сферах деятельности, были посвящены работы таких ученых, как А.М. Абрамов, А.И. Гуров, К.Э. Добрынин, А. Дьячков, Л.А. Ермакова, М.В. Кравченко, Ю.Г. Корухов, Б.А. Куринов, В.Д. Ларичев, С.В. Максимов, В.П. Шейнов, Г.М. Спирин и др.

Общие теоретические положения, которые могут быть положены в основу расследования мошенничества в сфере компьютерной информации, по производству отдельных следственных действий, использованию специальных знаний нашли отражение в трудах известных ученых: Т.В. Аверьяновой, О.Я. Баева, Р.С. Белкина, А.Н. Васильева, Т.С. Волчецкой, А.Ф. Волынского, В.К. Гавло, Ю.П. Гармаева, Л.Я. Драпкина, Н.Н. Егорова, В.Ф. Ермоловича, В.Д. Зеленского, Е.П. Ищенко, Ю.Г. Корухова, А.М. Кустова, В.П. Лаврова, Г.М. Меретукова, В.А. Образцова, А.А. Протасевича, Е.Р. Россинской, Н.А. Селиванова, Л.А. Соя-Серко, Д.А. Степаненко, А.И. Усова, Н.Г. Шурухнова, Н.П. Яблокова и др.

Отдельные вопросы расследования хищений с использованием компьютерной информации изучали ученые В.В. Крылов «Основы криминалистической теории расследования преступлений в сфере информации» (1998), В.А. Мещеряков «Преступления в сфере компьютерной информации: основы теории и практики расследования» (2002), «Основы методики расследования преступлений в сфере компьютерной информации» (2001), Ю.В. Гаврилин «Преступления в сфере ком-

пьютерной информации: квалификация и доказывание» (2003), Н.Г. Шурухнов «Расследование неправомерного доступа к компьютерной информации» (2004), В.Б. Вехов «Тактические особенности расследования преступлений в сфере компьютерной информации» (2004), Р.А. Белевский «Методики расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ» (2006) и другие.

В 2012 г. Р.С. Атамановым была защищена диссертация «Основы методики расследования мошенничества в сети Интернет», посвященная созданию общей методике расследования интернет-мошенничеств, раскрытию эффективных схем взаимодействия следователя с судебными экспертами, специалистами, органами, осуществляющими оперативно-розыскное сопровождение.

В 2015 г. А.С. Вражнов защищает диссертацию «Криминалистический риск при расследовании неправомерного доступа к компьютерной информации», в которой рассматривает типичные криминалистические ситуации, возникающие в процессе расследования неправомерного доступа к компьютерной информации, показывает взаимосвязь криминалистического риска с ситуацией информационной неопределенности в криминалистике, разрабатывает методические рекомендации по минимизации криминалистического риска в деятельности участников уголовного судопроизводства.

В 2016 г. Е.С. Шевченко была защищена диссертация «Тактика производства следственных действий при расследовании киберпреступлений», где автором рассмотрены проблемы организации и производства вербальных и невербальных следственных действий, направленных на получение виртуальной информации, показана необходимость использования криминалистического распознавания в ходе расследования киберпреступлений.

Простое перечисление научных трудов, посвященных расследованию преступлений в сфере компьютерной информации, показывает всё нарастающий и закономерный интерес ученых к этому преступлению с целью определить его понятие, выделить признаки, сформулировать единый терминологический аппарат, создать адекватную времени методику расследования, разработать криминалистические приёмы, алгоритмы, программы поисково-познавательной деятельности с целью повышения качества выявления, раскрытия, расследования и предупреждения данного вида преступлений. Имеющиеся сегодня научные положения составляют методологическую базу современных исследований, которые в свою очередь продолжают развивать высказанные ранее идеи, конкретизируя их при разработке частных методик расследования того или иного вида компьютерных преступлений.

В формирующейся методике расследования мошенничества в сфере компьютерной информации необходимо уделить внимание разработке актуальной криминалистической характеристики, раскрытию механизма преступления, определению специфики производства следственных действий, выбора формы использования специальных знаний.

Указанные обстоятельства и обусловили необходимость самостоятельного исследования следственной и судебной практики, анализа научных изысканий по данной проблематике и разработки на их основе, криминалистических рекомендаций по расследованию мошенничества в сфере компьютерной информации.

Объектом диссертационного исследования является преступная деятельность лиц, совершающих мошенничество в сфере компьютерной информации и поисково-познавательная деятельность лиц, ведущих расследование данного вида преступлений.

Предметом диссертационного исследования являются закономерности совершения мошенничества в сфере компьютерной информации, механизма данного преступления, возникновения информации о преступлении и его участниках, а также закономерности собирания, исследования, оценки и использования доказательств в расследовании обозначенных преступлений.

Целью диссертационного исследования является рассмотрение теоретических и практических вопросов формирующейся методики расследования мошенничества в сфере компьютерной информации, и разработка научно обоснованных криминалистических рекомендаций и рациональных способов организации раскрытия и расследования данного вида преступлений, отвечающих современному уровню развития информационных технологий, достижений криминалистической науки, общей теории судебных экспертиз.

Цель исследования предопределила необходимость постановки следующих исследовательских задач:

изучить состояние следственной и судебной практики по уголовным делам о мошенничестве в сфере компьютерной информации;

выявить и систематизировать проблемные зоны в расследовании указанных преступлений;

проанализировать современное состояние кибернетических, экономических, криминалистических, судебно-экспертных знаний, имеющих отношение к расследованию мошенничества в сфере компьютерной информации;

провести анализ некоторых научных категорий, относящихся к теме исследования: «криминалистическая характеристика преступления», «механизм преступления», «виртуальный след» и др.;

разработать актуальную криминалистическую характеристику мошенничества в сфере компьютерной информации как необходимого элемента формирования методики расследования преступлений данного вида, разработки методических рекомендаций;

проанализировать имеющиеся классификации следов мошенничества в сфере компьютерной информации;

построить информационную модель механизма мошенничества в сфере компьютерной информации;

определить задачи первоначального этапа расследования;

выявить типичные следственные ситуации мошенничества в сфере компьютерной информации;

разработать тактику производства отдельных следственных действий в зависимости от типичных исходных следственных ситуаций, последовательно складывающихся на первоначальном этапе расследования;

конкретизировать теоретические положения и практические рекомендации применения специальных знаний в процессе расследования мошенничества в сфере компьютерной информации;

рассмотреть актуальные вопросы назначения и проведения разных видов судебных экспертиз, необходимых при расследовании мошенничества в сфере компьютерной информации;

определить основные направления и порядок взаимодействия подразделений и служб правоохранительных органов при расследовании уголовных дел изучаемой категории.

Методология и методы научного исследования. Диссертационное исследование базируется на диалектическом методе научного познания объективной действительности, с позиции которой объект и предмет исследования рассматривались в развитии и взаимосвязи, взаимообусловленности, взаимопроникновении социальных и правовых явлений.

Методологической базой диссертационного исследования является совокупность различных методологических приемов, средств познания и эмпирического исследования. Так, применялись и использовались общие и частнонаучные методы познания: формально-логический, системно-структурный, анализ (изучение отдельных норм и положений нормативно-правовых актов, регламентирующих особенности деятельности в сфере компьютерной информации и ответственности за их нарушение, а также особенностей деятельности должностных лиц, осуществляющих расследование нарушений в указанной сфере); ситуационный; обобщение и описание (обобщение полученных статистических и иных данных, описание их влияния на процесс расследования рассматриваемой категории преступлений); метод анкетирования и интервьюирования (получение по разработанным анкетам необходимых для анализа и обобщения сведений); моделирование (создание условной модели деятельности отдельных категорий лиц, участвующих в совершении преступления, а также их поведения в процессе его расследования); статистический (при изучении официальной статистки, исторических фактов и т.п.); сравнение (влияние особенностей деятельности лиц, совершающих мошенничество в сфере компьютерной информации и лиц, осуществляющих их расследование) и иные методы.

Теоретическую основу диссертационного исследования составляют научные труды в области криминалистики, уголовного процесса, оперативно-розыскной деятельности, криминологии и психологии.

Нормативно-правовой основой исследования стали положения Конституции Российской Федерации; нормы действующего уголовного и уголовно-

процессуального законодательства; федеральные законы; ведомственные и межведомственные приказы и инструкции Генеральной прокуратуры Российской Федерации, Министерства юстиции Российской Федерации, Министерства внутренних дел Российской Федерации.

Эмпирическая база исследования. В процессе исследования изучено 217 уголовных дел о преступлениях в сфере компьютерной информации, в том числе мошенничества в сфере компьютерной информации, расследованных в г. Москве, Иркутской, Тверской, Тюменской, Ульяновской областях, Краснодарском, Читинском и Хабаровском краях, по которым осуществлялось предварительное расследование в период с 2004 по 2016 гг.

По специально разработанной анкете опрошено 192 сотрудника правоохранительных органов (следователей – 96, оперативных сотрудников – 78, экспертов – 18).

Эмпирическую базу исследования также составили статистические данные, характеризующие условия и результаты деятельности правоохранительных органов России и опубликованные материалы следственной практики.

Обоснованность и достоверность результатов исследования обеспечивается его методологией и методикой, а также репрезентативностью эмпирического материала, на котором основываются разработанные научные предложения и выводы.

Научная новизна исследования заключается в том, что, оно является специальным монографическим исследованием, посвященным формирующейся методике расследования мошенничества в сфере компьютерной информации и, в частности, первоначального его этапа.

Автором дано определение понятия и актуализировано содержание криминалистической характеристики мошенничества в сфере компьютерной информации, определен объективный характер связей и взаимообусловленностей между ее элементами, построена информационная модель механизма указанного вида преступления, рассмотрены организационные и методические аспекты первоначального этапа расследования, тактико- и технико-криминалистические особенности проведения следственных действий, определены наиболее продуктивные формы использования специальных знаний. Всё это является основой для разработки современной и эффективной методики первоначального этапа расследования мошенничества в сфере компьютерной информации.

Научная новизна также нашла своё отражение в разработке научно обоснованных методических рекомендаций по расследованию мошенничества в сфере компьютерной информации и определении их места в методике расследования преступлений данного вида. Автором предложены типовые программы, использование которых может повысить эффективность и качество расследования мошенничества в сфере компьютерной информации.

Основные положения, выносимые на защиту:

1. Объективной особенностью разработки методических рекомендаций расследования мошенничества в сфере компьютерной информации является специфи-

ческий объект (точнее объекты) познания. С одной стороны – мошенничество, определяемое законодателем как хищение чужого имущества или приобретение права на чужое имущество, с другой стороны – виртуальная среда, в которой эта преступная деятельность осуществляется путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, и в которой это преступление отражается в виде специфической следовой информации. Именно в таком виде объект исследования, имеет определяющее значение в формировании криминалистически значимой информации о данном виде преступлений.

2. Криминалистическая характеристика мошенничества в сфере компьютерной информации представляет собой обобщенное описание системы криминалистически значимой информации о признаках и свойствах преступления, предусмотренного ст. 159. 6 УК РФ, состоящее из определенного множества элементов, таких как: непосредственный предмет преступного посягательства; способ совершения преступления, орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые в свою очередь, характеризуются корреляционной зависимостью между собой, и специфичностью проявлений во внешней среде (киберпространстве), что и отличает данный вид преступной деятельности от схожих видов преступлений, и позволяет служить основанием для выдвижения типичных версий о событии преступления и личности преступника, определения направления поиска и познания лица, ведущего расследование.

3. Информационная модель механизма преступления – научная абстракция, позволяющая описать типичные существенные (криминалистически значимые) свойства, состояния, процессы преступного события в виде обобщенных сведений об участниках преступления, их действиях (бездействиях), обстановке преступления, а также закономерных связях, зависимостях между ними, о факторах и условиях внешней среды, влияющих на разворачивание преступного события и формирование следовой картины, с целью вооружения следователя комплексным системным знанием, способствующим оптимизации процесса расследования. Такая модель выполняет несколько функций: *познавательную*, так как она формулирует новое знание об исследуемом объекте; *объяснительную* – объясняет суть происходящих в процессе преступного события изменений; *инструментальную* – модель является средством моделирования и мысленного экспериментирования, что позволяет определить отклик системы на то или иное воздействие как элементов системы между собой, так и факторов внешней среды; *прогностическую* – прогнозирование динамики изменений в исследуемом объекте, связанных с развитием информационных технологий и телекоммуникационных систем.

4. Предложена авторская классификацию типичных следов мошенничества в сфере компьютерной информации: 1) традиционные следы (следы человека в местах нахождения конкретного лица в момент совершения преступления (следы

пальцев рук на клавиатуре и других компьютерно-технических средствах, внешний облик при встречи с жертвой преступления или при совершении преступниками подготовительных действий, например, при заключении договора об услугах провайдера и т.п.); используемых транспортных средств; средств связи и т.п.; 2) компьютерные следы, которые при любых действиях с компьютерными или иными программируемыми устройствами (мобильными телефонами, смартфонами, планшетами и т.д.) получают свое отображение в памяти.

5. Возбуждению уголовных дел о мошенничестве в сфере компьютерной информации предшествует предварительная проверка, направленная на выявление признаков состава преступления, специфичных только для данного вида преступлений. Эта специфика заключается в том, что для их выявления необходимо производство ряда организационно-проверочных, оперативно-розыскных, процессуальных действий, с соблюдением строго определенных правил, позволяющих изымать доказательственную и иную информацию из технических средств без потерь и искажений. Для этого обязательно применение компьютерных и иных технических средств, что предполагает своевременную организацию активного взаимодействия с соответствующими подразделениями, сотрудники которых обладают специальными знаниями в данной области, а также имеют в своем распоряжении необходимые средства.

6. Тактика производства следственных действий обусловлена: 1) спецификой механизма совершения мошенничества в сфере компьютерной информации; 2) применяемыми и используемыми для этого компьютерно-техническими средствами и программным обеспечением; 3) наличием информации о квалификации (характере знаний, умений и навыков) у лица (лиц), подозреваемого в совершении преступления; 4) поведением подозреваемого (например, наличие опыта общения с представителями правоохранительных органов и противодействия расследованию); 5) следственной ситуацией на момент проведения следственного действия.

7. Наиболее востребованными формами использования специальных знаний в процессе расследования мошенничества в сфере компьютерной информации являются следующие: назначение и производство судебных экспертиз; участие специалиста в производстве следственных действий; справочно-консультационная деятельность лица, обладающего специальными знаниями; допрос сведущего свидетеля. На первоначальном этапе расследования данного вида преступлений из всего комплекса возможных судебных экспертиз, необходимо прибегнуть к возможностям следующих классов (видов экспертиз): компьютерные экспертизы (аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая); экономических экспертиз (бухгалтерская); криминалистических экспертиз (техническая экспертиза документов, и в ряде случаев – трасологическая экспертиза).

Теоретическая и практическая значимость диссертационного исследования заключается в том, что на основе криминалистического учения о механизме преступления, а также анализа некоторых современных категорий криминалистики

– «криминалистическая характеристика преступления», «информационная модель механизма преступления», «следственная ситуация», «типовые программы расследования», «виртуальный след», «компьютерная информация», «киберпространство» и других, предпринята попытка теоретического осмысления их сущности и функционального назначения, определения путей повышения эффективности частной криминалистической методики расследования мошенничества в сфере компьютерной информации

В диссертации содержатся практические рекомендации, сформулированные на основе всестороннего изучения научных трудов и проведенного анализа судебной и следственной практики и направленные на совершенствование и оптимизацию деятельности лиц, ведущих расследование. Предложения и выводы, содержащиеся в работе могут быть использованы в дальнейших научных разработках проблем, связанных с раскрытием и расследованием мошенничества в сфере компьютерной информации.

Кроме этого, полученные результаты могут быть использованы в учебном процессе высших учебных заведений при преподавании криминалистики, общей теории судебных экспертиз, при проведении занятий на курсах повышения квалификации, а также использованы в практической деятельности сотрудников правоохранительных органов.

Апробация результатов исследования и внедрение. Наиболее важные аспекты исследуемой проблемы изложены в 16 научных публикациях, в том числе 4 статьи в рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией Министерства образования и науки Российской Федерации, а также авторские разделы в двух коллективных монографиях по теме исследования (общим объемом 9 п.л.). Автор участник двух грантов по исследуемой проблематике.

Результаты диссертационного исследования обсуждались на заседаниях кафедры криминалистики, судебных экспертиз и юридической психологии Байкальского государственного университета, а также различных международных, всероссийских и вузовских научно-практических конференциях, круглых столах.

Основные результаты, полученные автором по результатам исследования и содержащиеся в материалах диссертации, внедрены в учебный процесс ФГБОУ ВО «Байкальский государственный университет», ФГКОУ ВО «Восточно-Сибирский институт Министерства внутренних дел Российской Федерации», в практическую деятельность отдела «К» ГУ МВД России по Иркутской области, Следственного управления Следственного комитета Российской Федерации по Иркутской области, в работу Прокуратуры Иркутской области.

Структура и объем работы. Структура диссертационного исследования обусловлена его целью и задачами. Диссертация состоит из введения, трех глав, объединяющих шесть параграфов, заключения, списка использованной литературы и приложений.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** аргументируется актуальность темы исследования, ее разработанность, определяется объект и предмет исследования, цель и задачи, теоретическая и практическая значимость, методологическая база исследования и методы, указывается эмпирическая база, достоверность научная новизна исследования, формулируются основные положения, выносимые на защиту, приводятся сведения об основных результатах исследования ее апробации и внедрения.

Глава 1 «Мошенничество в сфере компьютерной информации как объект криминалистического анализа» состоит из двух параграфов.

Первый параграф **«Общие положения криминалистической характеристики мошенничества в сфере компьютерной информации»** посвящен основным наиболее информативным элементам криминалистической характеристики мошенничества в сфере компьютерной информации, их взаимосвязи и взаимообусловленности. К таким элементам относятся: способ совершения преступления, компьютерные средства совершения преступления, место и обстановка совершения преступной деятельности, механизм следообразования, а также влияние каждого из них на механизм преступления.

На первоначальном этапе расследования следственные органы, как правило, не располагают сведениями о компьютерных средствах, используемых в преступлении. Поэтому выделение такого структурного элемента как средства преступления и его взаимосвязи со способом преступления и личностью преступника даёт основание для построения первоначальных версий расследования и определения направления поиска.

Выбор средства зависит от объекта посягательства, применяемых технических и организационных средств охраны, защиты информации.

Преступления совершаются различными способами с применением специальных программно-аппаратных средств и сетевых технологий. Способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также новых или модифицированных программ. Вопрос о компьютерных средствах в качестве орудий преступления малоизучен. Понятие компьютерное средство является комплексным и включает в себя компьютеры в различных вариантах их исполнения, компьютерные технологии, компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение. Сегодня главную роль при совершении исследуемых преступлений играет программное обеспечение, а не аппаратные средства, которые сами по себе не представляют опасности.

Наличие компьютерных средств является обязательным, именно они предопределяют специфичность способов совершения мошенничества в сфере компьютерной информации.

Познание такого явления, как мошенничество в сфере компьютерной информации заключаются в изучении, с одной стороны – мошенничества в общем виде, с другой – среды, в которой оно находит свое отражение. Данная среда представляет собой виртуальное пространство (киберпространство), граничащее с объективной реальностью. Это обстоятельство имеет определяющее значение для разработки научных положений и практических рекомендаций по расследованию мошенничества в сфере компьютерной информации.

Указывая на сложный характер, рассматриваемой преступной деятельности, автор отмечает, что способ совершения мошенничества имеет полноструктурное строение, состоит из подготовки к совершению мошенничества, реализации самого способа совершения, а также деятельности направленной на сокрытие следов преступления. На этапе подготовки, преступники осуществляют деятельность, направленную на сокрытие следов преступления, которая выражается в создании вредоносных программ, позволяющих проникать в компьютер жертвы без информирования ее об этом, удаленный доступ в компьютер жертвы или общение с ней на значительном расстоянии с использование различных программ.

Способ совершения преступлений зависит от подбора компьютерных средств, а также лиц, которые в зависимости от распределенной им роли, выполняют возложенные на них обязанности по совершению мошенничества в виртуальном пространстве. Указанные лица не всегда могут знать об истинных целях их деятельности (разработка программы, которая в последующем может быть использована в качестве вредоносной, курьерские услуги и т.п.).

Следовая картина мошенничества в сфере компьютерной информации обусловлена спецификой образования, обработки и хранения компьютерной информации, предусматривающей использования для этих целей вполне материальных средств (компьютерно-технических). Это обстоятельство предусматривает возможность материально-фиксированного отображения компьютерной информации на носителях указанных средств. В целях выявления, изъятия и исследования компьютерной информации, даже с учетом ее блокирования или уничтожения и т.п., изъятию подлежит жесткий диск, а также другие компьютерные средства для обнаружения следов такой деятельности, самой компьютерной информации и их извлечения.

Собрав и проанализировав данные следственной и судебной практики, а также мнения ученых, автор предлагает следующую классификацию типичных следов мошенничества в сфере компьютерной информации:

традиционные следы: следы человека в местах нахождения конкретного лица в момент совершения преступления (отпечатки пальцев рук на клавиатуре и других компьютерно-технических средствах, внешний облик при встречи с жертвой преступления или при совершении преступниками подготовительных действий, например, при заключении договора об услугах провайдера, по записи камеры видеонаблюдения…); следы используемых транспортных средств; средств связи и т.п.

компьютерные следы, как «любые изменения состояния автоматизированной информационной системы, связанные с событием преступления и зафиксированные в виде компьютерной информации» (Мещеряков В.А., 2001).

Важное значение имеют данные о месте возможного обнаружения следов рассматриваемого деяния. Рассматривая характерные особенности функционирования компьютерной сети, автор делает вывод о том, что с одной стороны, местом совершения мошенничества в сфере компьютерной информации является сама информационно-телекоммуникационная сеть, в которой происходит ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, а с другой стороны, местом совершения мошенничества в сфере компьютерной информации является местонахождение конкретного компьютера, с которого осуществляется неправомерный доступ, именно в этом месте находится основной объем информации, характеризующий процесс совершение преступления (способ, орудия и средства, место, время, обстановка), следовая информация. В процесс совершения преступления для обмена информацией в целях извлечения сведений дополнительно будет вовлечено, как минимум ещё одно, или нескольких устройств. Большинство таких преступлений совершается на удаленном доступе по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение. Приходится констатировать, что такое положение негативно сказывается на процессе выявления, раскрытия и расследования мошенничества, особенно в тех случаях, когда неправомерный доступ к информации осуществляется из-за рубежа. Кроме телекоммуникационной сети, реального места нахождения компьютера (дополнительных устройств), местом совершения мошенничества является и место, «обналичивания» денежных средств, полученных путем обмана (процесс легализации материальных ценностей значительно влияет на характер следообразования).

Наиболее определяющими по делам о мошенничестве в сфере компьютерной информации являются данные о местонахождении компьютерно-технического средства (средств), принадлежащего жертве и подвергшегося воздействию со стороны субъекта преступной деятельности. Обусловлено это тем, что именно указанные компьютерно-технические средства в первую очередь попадают в поле зрения следователя и от грамотного обращения с ними зависит весь ход дальнейшего расследования. В большинстве случаев указанные средства являются единственными носителями первоначальной криминалистически значимой информации.

На основании проведенного анализа автором подчеркивается двойственное значение компьютерных средств, как следообразующих объектов, которые проявляются в двух аспектах, как носители информации об объективной стороне преступного деяния и, как носители информации о самом субъекте преступления. Характерная особенность этого заключается в том, что компьютерные средства

сами не выступают следами преступной деятельности, так как не обладают характерными специфическими признаками, но при этом они несут на себе следовую картину преступного деяния.

Во втором параграфе **«Информационная модель механизма совершения преступления, его соотношение с криминалистической характеристикой»** дается понятие и предлагается структура информационной модели механизма мошенничества в сфере компьютерной информации.

Основными элементами модели механизма мошенничества в сфере компьютерной информации являются: 1) деятельность субъекта преступления – мошенника, осуществляющего хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (обман или злоупотребление доверием, как правило, характерен на этапе подготовки к преступлению) в киберпространстве; 2) совокупность действий, поступков жертвы мошенничества, совершенного в сфере компьютерной информации; 3) совокупность действий, поступков лиц, оказавшихся косвенно связанных с преступным событием; 4) элементы обстановки, используемые участниками преступного события, включая предмет преступного посягательства.

Характерной особенностью мошенничества в сфере компьютерной информации является то, что способ совершения преступной деятельности находится в неразрывной связи с особенностями личности субъекта этой деятельности, который на первоначальном этапе остаётся, как правило, неизвестным. При этом, автор отмечает, что, свойства и качества личности компьютерного мошенника закономерно формируются под воздействием многообразных условий социальной среды и являются относительно устойчивыми.

Не менее важной особенностью, отмеченной автором в процессе создания модели механизма мошенничества в сфере компьютерной информации, по мнению автора, является использование субъектом преступной деятельности имеющихся у него компьютерных средств, а также обязательное их подключение к компьютерной сети в целях совершения преступления. Это обстоятельство, по мнению автора, обусловило выделение законодателем такого преступления в отдельный вид – компьютерного мошенничества.

Положив в основу создания модели механизма мошенничества в сфере компьютерной информации предложенные выше особенности, автор предлагает всех преступников классифицировать в зависимости от уровня знания, владения и умения пользоваться программным обеспечением и технически сложными устройствами, в частности компьютерно-техническими средствами. В этой связи следует различать:

1) профессиональных субъектов преступной деятельности («хакеров», «компьютерных злоумышленников»), которые являются программистами высшего

класса (IT-специалистами) и работают либо с уже реализованными программами, либо придумывают уникальные программы самостоятельно.

2) непрофессиональных субъектов преступной деятельности (могут иметь специальное образование или относится к «самоучкам»). Они в свою очередь делятся на:

а) продвинутых пользователей (могут создавать несложные компьютерные программы, сайты, понимают всю механику действия и работы на технически сложных устройствах и ПК);

б) уверенных пользователей (знают, как работают компьютерные системы, могут сами устанавливать компьютерные программы).

По основанию – доступ к компьютерным сетям – всех субъектов преступной деятельности разделить на лиц, профессиональная деятельность и сфера работы которых связана со свободным доступом к компьютерным средствам и сетям и лиц, которые осуществляют преступную деятельность, используя собственные компьютерные средства в домашних условиях. Имеется отдельная категория преступников, которые используют возможности доступа к сети интернет в местах общего пользования (кафе, рестораны, бары, транспорт, вокзалы, аэропорты, иные организации со свободным доступом к интернету через сеть WI-FI).

По количественному составу данных субъектов: 1) совершенное одним лицом; 2) группой лиц по предварительному сговору; 3) организованной преступной группой лиц (преступным сообществом).

Количественный и качественный состав лиц, участвующих в совершении мошенничества в сфере компьютерной информации в значительной степени влияет на выбор орудий и средств совершения преступления.

Автор отмечает, что все элементы механизма мошенничества в сфере компьютерной информации, оказывают взаимообратное воздействие друг на друга. Это, в частности, вытекает из того, что профессиональная квалификация субъектов мошенничества обусловливает выбор способа его совершения, а также орудий и средств, используемых в этих целях. Чем выше квалификация субъектов преступной деятельности, тем более изощренные приемы и средства применяются в ходе совершения преступной деятельности. Именно это обстоятельство обусловливает взаимосвязь криминалистической характеристики и механизма мошенничества в сфере компьютерной информации.

Одним из основных элементов, оказывающих определяющее значение для разработки практических рекомендаций расследования мошенничества в сфере компьютерной информации, является поведение жертвы преступной деятельности. Обусловлено это тем, что уже на этапе подготовки, преступники осуществляют деятельность, направленную на сокрытие следов преступления. Именно это обстоятельство оказывает влияние на создание методических рекомендаций по раскрытию и расследованию мошенничества в сфере компьютерной информации.

Глава 2 **«Особенности первоначального этапа расследования мошенничества в сфере компьютерной информации»** состоит из двух параграфов.

В первом параграфе **«Особенности возбуждения уголовных дел о мошенничестве в сфере компьютерной информации и первоначальный этап расследования»** в результате исследования автором выявлено, что по уголовным делам о мошенничестве в сфере компьютерной информации во всех случаях расследования дел указанной категории возбуждению уголовного дела предшествовала предварительная проверка. Обусловлено это рядом объективных причин. Признаки совершенного мошенничества в сфере компьютерной информации (объективные и субъективные), как правило, не ярко выражены. Их обнаружение требует выполнения достаточно сложных и последовательных следственных и иных процессуальных действий, в целях придания доказательственного значения получаемой криминалистически значимой информации, свидетельствующей о совершенном преступлении. На весь процесс деятельности следователя или лица, производящего дознание оказывает влияние ситуация, складывающаяся на момент получения информации о событии (условно назовем ее следственной). Обусловлено это источниками и характером полученной информации.

Автор установил, что на выбор средств предварительной проверки оказывают влияние две типичные (проверочные) ситуации.

1. Преступники продолжают совершать незаконные действия, и существует устойчивая связь между ними и лицом, в отношении которого совершается компьютерное мошенничество.

2. Преступление окончено и связь между лицом, в отношении которого оно совершено и мошенниками отсутствует.

Наибольший объем первичной информации, о совершенном мошенничестве в процессе проведения предварительной проверки всегда поступает из объяснений различных категорий лиц. После опроса лиц, обладающих сведениями о совершенном (совершаемом) преступлении необходимо незамедлительно преступить к осмотру места нахождения компьютерно-технических средств или иных технически сложных устройств, послуживших средствами совершения мошенничества, находящихся в распоряжении пострадавшего лица. Для установления оснований возбуждения уголовного дела одним из основных средств разрешения данных ситуаций является возможность и необходимость назначения и производства компьютерной экспертизы, а также других видов экспертиз. В целях сбора объектов, являющихся следами или их носителями, в ходе предварительной проверки по делам о мошенничестве в сфере компьютерной информации должны быть истребованы и изъяты различные документы. Они могут быть изъяты в ходе производства осмотра места происшествия, проведения документальных проверок или ревизий, а также могут быть истребованы на основании письменного постановления должностного лица, производящего проверку. Во всех случаях при

производстве следственных и иных процессуальных действий при расследовании мошенничества в сфере компьютерной информации целесообразно присутствие специалиста, обладающего знаниями в области компьютерно-технических средств, а также активное взаимодействие с иными подразделениями.

Автор делает вывод о том, что при производстве проверочных действий необходимо учитывать, что полученные в ходе нее доказательства должны в полной мере использоваться в ходе дальнейшего расследования, а отдельные из них, в последующем другими способами получить вообще невозможно. Это следует учитывать при проведении проверки по делам о мошенничестве в сфере компьютерной информации. Во всех случаях результаты предварительной проверки оказывают влияние на формирование следственных ситуаций первоначального этапа расследования мошенничества в сфере компьютерной информации и механизма их разрешения.

Во втором параграфе **«Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования мошенничества в сфере компьютерной информации»** определяется перечень следственных действий первоначального этапа расследования, рассматривается специфика их производства, формулируются рекомендации по тактико-криминалистическому обеспечению.

Следственные действия являются познавательным инструментарием лица, ведущего расследование, и универсальными средствами получения доказательств. Их производство обусловлено необходимостью получения уголовно-релевантной информации, имеющей значение для установления обстоятельств расследуемого преступного события, составляющих предмет доказывания по уголовному делу. Исследование теоретических аспектов расследования мошенничеств в сфере компьютерной информации требует понимания таких категорий как «компьютерная информация», «кибернетическое пространство», «виртуальный след», так как поисково-познавательная деятельность следователя будет осуществляться относительно этой информации в соответствующем пространственно-временно континууме.

Автор определяет, что в зависимости от механизма преступной деятельности и складывающихся на первоначальном этапе расследования мошенничества в сфере компьютерной информации следственных ситуаций наиболее целесообразно проведение следующих следственных действий: осмотра места происшествия, осмотра предметов и документов; допроса лиц, процессуальное положение которых определено; обыска и выемки; получение образцов для сравнительного исследования; назначение таких судебных экспертиз, как компьютерные экспертизы; технической экспертизы документов; трасологической экспертизы; бухгалтерской экспертизы.

Рассматривая тактику производства отдельных следственных действий, автор отмечает, что производство допроса по уголовным делам этой категории напрямую зависит от специфики механизма совершения преступления данного ви-

да и иных как позитивных, так и негативных факторов. К числу первых следует отнести наличие определенного объема информации о преступном событии, полученного из различных источников (в ходе предварительной проверки материалов о расследуемом событии, результаты оперативно-розыскных мероприятий и т.п.), а также информации о лице, с которым предстоит производство следственного действия (полученной ранее в ходе его объяснений, из протоколов процессуальных действий и т.д.). В число негативных факторов можно включить значительный промежуток времени, прошедший с момента совершения мошенничества до момента производства допроса. Кроме этого, содержание самого механизма преступного деяния таково, что при выяснении всех его элементов и обстоятельств совершения, требуется наличие знаний о специфике мошенничества в сфере компьютерной информации, которые в свою очередь зависят от применяемых для его реализации орудий и средств – компьютеров, технически сложных устройств, накопителей информации, компьютерных сетей и доступа к ним и др. Эти обстоятельства в первую очередь обусловливают при производстве следственных действий (в данном случае при допросе) необходимость привлечения специалиста в сфере компьютерных технологий.

Автором установлено, что по уголовным делам о мошенничестве в сфере компьютерной информации, осмотр места происшествия производится с целью выявления: компьютерных следов, а также их объектов – носителей (например, компьютера или системного блока, флеш-накопителей и т. п.); традиционных следов присутствия конкретного лица на месте происшествия; особенностей доступа, организации, функционирования и устройства различных видов сетей, посредством использования которых было совершено мошенничество; устройств регистрации и видео фиксации, имеющихся на территории учреждения, либо прилегающей территории к месту совершения преступления и т.п. Это обстоятельство определяет выбор тактических, методических, технико-криминалистических и организационных средств, способствующих обнаружению, фиксации и изъятия специфических следов мошенничества в сфере компьютерной информации.

Автор обращает особое внимание на то, что во всех случаях производства осмотра места происшествия, а также других следственных и процессуальных действий, следователь обязан помнить о том, что на компьютерно-технических средствах, подлежащих исследованию, могут быть установлены специальные защитные программы, которые без требуемого командного уведомления (пароля) приступают к уничтожению информации. В целях нейтрализации указанной ситуации целесообразно получать доступ к таким паролям путем добровольной выдачи лицами, обладающими ими. Только в этом случае существует возможность изъять компьютерную информацию, осуществить копирование документов, имеющих отношение к расследуемому мошенничеству. В противном случае несоблюдение указанных тактических особенностей производства осмотра места происшествия и других процессуальных действий может привести к ее

безвозвратной потере необходимой для расследования информации. Во всех случаях мошенничества в сфере компьютерной информации при производстве осмотра места происшествия и иных следственных действий, необходимо учитывать текущее состояние компьютерно-технических средств, а также времени, прошедшего с момента совершения преступления до момента их производства.

Всесторонний проведенный анализ позволяет автору констатировать, что производство обыска, по делам о мошенничестве в сфере компьютерной информации, может носить неотложный характер, тогда как выемка производится по результатам предварительного установления точного места нахождения предметов (документов), содержащих информацию, в том числе компьютерную, или же по желанию лица выдать их следователю добровольно. При производстве обыска или выемки по уголовным делам рассматриваемой категории, рекомендуется изымать все технические устройства и средства, связанные с возможностью доступа к компьютерным сетям (особенно это касается сети Интернет), которые могли быть использованы при подготовке к совершению мошенничества и сокрытию его следов, также необходимо изымать все электронные средства хранения информации, как потенциальные источники, на которых может храниться программное обеспечение или его элементы.

Автор отмечает, что во всех случаях, при производстве любых следственных действий по делам о мошенничестве в сфере компьютерной информации необходимо использовать различные формы специальных знаний с учетом извлечений, установленных автором в процессе их применения.

Глава 3 **«Использование специальных знаний как условие оптимизации и качественного расследования мошенничества в сфере компьютерной информации»** состоит из двух параграфов.

Первый параграф **«Формы использования специальных знаний при расследовании мошенничества в сфере компьютерной информации»**

Особенностью расследований в сфере компьютерной информации является, прежде всего, необходимость использования специальных знаний в области информационных технологий не только при проведении экспертизы, но и при производстве следственных действий (осмотре, обыске, выемки) для поиска, обнаружения, фиксации, изъятия и представления на экспертизу материальных объектов – носителей информации.

Проведенное автором исследование показало, что наиболее востребованными формами использования специальных знаний в процессе расследования мошенничества в сфере компьютерной информации являются следующие: назначение и производство судебных экспертиз; участие специалиста в производстве следственных действий; справочно-консультационная деятельность лица, обладающего специальными знаниями; допрос сведущего свидетеля.

В работе предлагается и другая классификация использования специальных знаний по делам о мошенничестве в сфере компьютерной информации:

1. При проведении предварительной проверки материалов до возбуждения уголовного дела:

а) при осуществлении оперативно-розыскной деятельности;

б) при производстве следственных действий, проведение которых возможно до возбуждения уголовного дела.

2. При производстве следственных и иных процессуальных действий при наличии уже возбужденного уголовного дела.

3. Назначение и производство судебных экспертиз.

Исходя из такой классификации, автором рассмотрены особенности применения и использования специальных знаний при расследовании рассматриваемого вида преступлений, подняты проблемы поиска высококвалифицированных специалистов, обладающих необходимыми познаниями в сфере высоких технологий. Процессуальный статус лица, привлекаемого в роли специалиста или эксперта зависит от конкретной следственной ситуации. Следователь, руководствуясь положениями УПК РФ и стоящими перед ним задачами, определяет, кого ему привлечь к участию в производстве следственных и иных процессуальных действий и в какой форме использовать специальные знания.

Второй параграф **«Судебные экспертизы при расследовании мошенничества в сфере компьютерной информации: виды, современные возможности, проблемы оценки следователем результатов экспертных исследований»**

Параграф посвящен рассмотрению современных возможностей производства относительно нового класса компьютерных экспертиз, а также традиционных классов судебных экспертиз: криминалистических, экономических.

На первоначальном этапе расследования данного вида преступлений из всего комплекса возможных судебных экспертиз, необходимо прибегнуть к возможностям следующих классов (видов экспертиз): компьютерные экспертизы (аппаратно-компьютерная; программно-компьютерная; информационно-компьютерная; компьютерно-сетевая); экономических экспертиз (бухгалтерская); криминалистических экспертиз (техническая экспертиза документов, и в ряде случаев – трасологическая экспертиза).

На основе проведенного исследования автором отмечается, что при расследовании мошенничества в сфере компьютерной информации в ряде случаев целесообразно назначение комплексного исследования, по результатам которого следователь может получить значительный объем информации о связях лиц, которые участвовали в совершении мошенничества, установить особенности механизма документооборота между сотрудниками учреждения, ставшего жертвой мошенников и самими преступниками, а также физическими лицами.

Для определения формы комплексного исследования, процессуальных и организационных аспектов его назначения и производства, формулирования вопросов экспертам, правильной оценке экспертного заключения следователь должен

уметь четко определять будет он назначать комплексную экспертизу или комплекс экспертиз.

В **Заключении** нашли отражение основные выводы и предложения, сформулированные в диссертационном исследовании.

В приложениях к диссертации представлены материалы, которые послужили обоснованием результатов проведенного исследования и выносимых на защиту положений.

Основные положения диссертации нашли отражение в следующих публикациях:

Статьи в ведущих рецензируемых научных журналах и изданиях, определенных Высшей аттестационной комиссией Министерства образования и науки Российской Федерации:

1. Коломинов, В.В. Допрос и участие в нем специалиста при расследовании мошенничества в сфере компьютерной информации / В.В. Коломинов // Вестник Московского государственного областного университета. Серия «Юриспруденция». – 2015. – №1. (0.5п.л.)
2. Коломинов, В.В. Мошенничество в сфере компьютерной информации: криминалистический аспект / В.В. Коломинов // Известия Иркутской государственной экономической академии: электронный научный журнал. – 2015. – Т. 6. – №1. (0.5 п.л.)
3. Коломинов, В.В. О способе совершения мошенничества в сфере компьютерной информации / В.В. Коломинов // Человек: преступление и наказание. – 2015. – №3(90). (0.4 п.л.)
4. Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации / И.Г. Смирнова, В.В. Коломинов // Известия Иркутской государственной экономической академии: электронный научный журнал. – 2015. – Т6. – № 3. (0.7 п.л.)

Иные научные статьи и публикации:

1. Коломинов, В.В. Мошенничество сфере компьютерной информации как объект криминалистического исследования / В.В. Коломинов. – М.: ИИУ МГОУ, 2013. (0.5 п.л.)
2. Коломинов, В.В. К вопросу о формировании криминалистического знания о мошенничестве в сфере компьютерной информации / И.Г. Смирнова, В.В. Коломинов // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства: материалы международной научно-практической конференции, Иркутск, 25-26 сентября 2014г. – Иркутск: Изд-во БГУЭП, 2014. (0.4 п.л.)
3. Коломинов, В.В. К вопросу об установлении места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации / В.В. Коломинов // Проблемы и перспективы современных

гуманитарных, экономических и правовых исследований: материалы пятой международной научно-практической конференции (г. Москва (Российская Федерация) – г. Милан (Италия) – 25 апреля – 3 мая 2014 г.): в 2-х ч. Ч. II / под ред. А.М. Кустова, Т.Ю. Прокофьевой. – М.: ИИУ МГОУ, 2014. (0.4 п.л.)

4. Коломинов, В.В. Киберпреступность в ряде стран Азиатско-Тихоокеанского региона: сравнительно-правовой анализ / И.Г. Смирнова, О.А. Егерева, В.В. Коломинов // Евразийская парадигма России и трансформация политико-правовых институтов стран Азиатско-Тихоокеанского региона: материалы пятой международной научно-практической конференции (Улан-Удэ, 19–21 июня 2014 г.) / науч. ред. Ю.И. Скуратов. – Улан-Удэ: Издательство Бурятского госуниверситета, 2014. (0.3 п.л.)

5. Коломинов, В.В. Некоторые аспекты формирования криминалистических знаний о мошенничестве в сфере компьютерной информации / В.В. Коломинов // Проблемы и перспективы современных гуманитарных, экономических правовых исследований: материалы шестой научно-практической конференции г. Москва – г. Мсида (Мальта) 6-9 октября 2014 г. – М.: ИИУ МГОУ, 2014. (0.3 п.л.)

6. Коломинов, В.В. К вопросу об окончании производства по уголовным делам в сфере компьютерных технологий: анализ судебной практики / И.Г. Смирнова В.В. Коломинов // Научные труды. Российская академия юридических наук. – М.: Юрист, 2015. (0.4 п.л.)

7. Коломинов, В.В. Кибертерроризм как угроза национальной безопасности государства / И.Г. Смирнова, В.В. Коломинов // Проблемы правотворческой и правоприменительной практики в условиях развития информационного общества: сборник научных статей: в 2-х ч., Ч .2 / ГрГУ им. Я. Купалы; редкол.: С.Е. Чебуранова. – Гродно: ГрГМУ, 2015. (0.2 п.л.)

8. Коломинов, В.В. Мошенничество в сфере компьютерной информации как объект криминалистического познания / В.В. Коломинов // Сибирские уголовно-процессуальные и криминалистические чтения. – 2015. – Вып. 2 (8). (0,4 п.л.)

9. Коломинов, В.В. Тактические особенности производства осмотра по делам о мошенничестве в сфере компьютерной информации / В.В. Коломинов // Уголовное производство: процессуальная теория и криминалистическая практика: материалы третьей международной научно-практической конференции. – Симферополь: КФУ им. В.И. Вернадского, 2015. (0.4 п.л.)

10. Коломинов, В.В. Установление места совершения преступления в процессе расследования мошенничества в сфере компьютерной информации / В.В. Коломинов // Криминалистические чтения на Байкале – 2015: материалы международной научно-практической конференции / отв. ред. Д.А. Степаненко. – Иркутск: Восточно-Сибирский филиал ФГБОУ ВО «РГУП», 2015. (0.4 п.л.)

Коллективные монографии:

11. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / под науч. ред. И.Г. Смирновой. – М.: Юрлитинформ, 2016. – 312 с. (авторский параграф 5.2) (2 п.л.)

12. Особенности расследования отдельных категорий уголовных дел и уголовных дел в отношении отдельных категорий лиц: монография / под науч. ред. И.Г. Смирновой. – М.: Юрлитинформ, 2016. – 336 с. (авторская глава 2.1) (1.3 п.л.)