На правах рукописи

**Атаманов Руслан Сергеевич**

**ОСНОВЫ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ**

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

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата юридических наук

Москва – 2012

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Московская государственная юридическая академия имени О.Е. Кутафина»

|  |  |
| --- | --- |
| **Научный руководитель:** | **Ищенко Евгений Петрович,**доктор юридических наук, профессор, Заслуженный деятель науки, Заслуженный юрист РФ |
| **Официальные оппоненты:** | **Волынский Александр Фомич,**доктор юридических наук, профессор, Заслуженный деятель науки, Заслуженный юрист РФ, профессор кафедры криминалистики Московского университета Министерства внутренних дел Российской Федерации" |
|  | **Захарова Валентина Олеговна,**кандидат юридических наук, доцент кафедры криминалистики Института повышения квалификации Следственного комитета Российской Федерации |
| **Ведущая организация:** | **Башкирский государственный университет** |

 Защита состоится 22 ноября 2012 г. в 12:00 на заседании диссертационного совета Д 212.123.01, созданного на базе Московской государственной юридической академии имени О.Е. Кутафина, 123995,
г. Москва, **улица Садовая-Кудринская, д. 9, зал заседаний диссертационного совета.**

 **С диссертацией можно ознакомиться в библиотеке Московской государственной юридической академии имени О.Е. Кутафина.**

**Автореферат разослан «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2012 г.**

**Учёный секретарь диссертационного совета**

доктор юридических наук, Г.А. Есаков
профессор

**Общая характеристика работы**

**Актуальность темы диссертационного исследования.** Высокие темпы развития информационных технологий, повсеместное внедрение разрабатываемых информационно-телекоммуникационных систем и технических средств во все сферы жизнедеятельности членов современного общества, растущее доверие к информационным системам со стороны населения, а также современное состояние систем защиты информации создало объективные предпосылки возникновения новой разновидности преступлений – преступлений в сфере высоких технологий, распространение которых неизбежно ставит сотрудников правоохранительных органов перед необходимостью детального изучения программно-технических возможностей современных компьютерных систем, их использования в борьбе с преступлениями в сфере высоких технологий.

Современные компьютерные системы охватывают практически все сферы социальной структуры, науки и, особенно, экономики. Доступность информационных ресурсов, высокая скорость обработки данных – всё это и многое другое способствует интеграции информационных технологий в жизнедеятельность человека. В этой связи борьба с преступностью в сфере высоких технологий и компьютерной информации приобрела характер международной проблемы и актуальна для деятельности правоохранительных органов практически во всех странах. В Российской Федерации достаточно длительное время отмечался рост данного вида преступлений. Так, по данным статистики МВД России, количество зарегистрированных преступлений в сфере компьютерной информации в 2003 году составило 7540, в 2004 — 8739, в 2005 — 10214, в 2006 — 8889, в 2007 — 7236, в 2008 г. — 9010, в 2009 г. — 11636, в 2010 — 7398, в 2011 — 2698, а за первые 4 месяца 2012 года — 1154[[1]](#footnote-1). Как видно, статистика демонстрирует волнообразную динамику развития преступности в сфере компьютерной информации и, в том числе преступлений, совершаемых в сети Интернет. С 2009 года наблюдается снижение числа зарегистрированных преступлений. С 2011 года темп спада снизился, в связи с чем есть основания полагать, что в ближайшие годы количество зарегистрированных преступлений в сфере компьютерной информации снова начнёт расти.

Среди известных на сегодняшний день преступлений, совершаемых в сети Интернет, особую опасность представляет интернет-мошенничество. В силу своей высокой латентности, а также трудности выявления и расследования, данное преступление нуждается во всестороннем научном исследовании.

Рост числа интернет-магазинов, создание систем предоставления банковских услуг посредством глобальной сети, развитие платёжных систем способствует тому, что всё больше и больше людей доверяют безналичным расчётам, забывая о том, что даже в виртуальных экономиках действуют криминальные схемы.

**Степень разработанности проблемы**. Современное состояние разработанности вопросов методики расследования мошенничества в сети Интернет характеризуется, с одной стороны, недостаточным интересом к данному виду преступлений, а с другой – большой теоретической и практической значимостью для практики борьбы с преступностью в сети Интернет. Всё это нашло своё отражение в работах В.Б. Вехова «Тактические особенности расследования преступлений в сфере компьютерной информации» (2004), Р.А. Белевского «Методики расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ» (2006), В.А. Мещерякова «Преступления в сфере компьютерной информации: основы теории и практики расследования» (2002), Т.П. Кесареевой «Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет» (2002), В.В. Крылова «Основы криминалистической теории расследования преступлений в сфере информации» (1998),
Н.Г. Шурухнова «Расследование неправомерного доступа к компьютерной информации» (2004) и других учёных.

Проблемы использования специальных познаний при расследовании преступлений в сфере высоких компьютерных технологий, к которым, в частности, относится интернет-мошенничество, были рассмотрены в работах А.И. Усова «Концептуальные основы судебной компьютерно-технической экспертизы» (2002), Е.Р. Россинской «Судебная компьютерно-техническая экспертиза» (2001), А.А. Шаевича «Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений» (2007), А.В. Нарижного «Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий» (2009), В.А. Мещерякова «Концептуальные основы судебной компьютерно-технической экспертизы» (2002), А.И. Семикаленовой «Судебная программно-компьютерная экспертиза по уголовным делам» (2005), О.В. Тушкановой «Особенности применения специальных познаний в области компьютерной информации на стадиях выявления, раскрытия и расследования преступлений» (2008),
А.Н. Яковлева «Информационные технологии и судебная экспертиза» (1999) и др.

Несмотря на большое количество публикаций, посвящённых расследованию преступлений, связанных с использованием компьютерной техники, появившихся в последнее время, вопросы методики расследования именно интернет-мошенничества практически не рассматривались. Большинство опубликованных на сегодняшний день работ по тематике преступлений в сфере высоких компьютерных технологий, если и упоминают о мошенничестве, то вскользь, чаще останавливаясь на исследовании таких преступлений, как неправомерный доступ к компьютерной информации.

Следует отметить, что существующие в настоящее время методические рекомендации по выявлению, раскрытию и расследованию корыстных преступлений, совершаемых в сети Интернет, далеко не всегда отражают всю специфику деятельности правоохранительных органов в этих целях. В большинстве случаев, они нацелены на проведение следственных действий при расследовании преступлений в кредитно-финансовой сфере.

В то же время существует объективная необходимость разработки методических рекомендаций, носящих комплексный характер, позволяющих повысить эффективность работы участников предварительного расследования при выявлении и расследовании интернет-мошенничества.

Таким образом, актуальность диссертационного исследования обусловлена, с одной стороны, высокой практической значимостью, а с другой – недостаточной научной разработанностью вопросов методики расследования мошенничества в сети Интернет.

**Объект и предмет исследования.** Объектом исследования является криминалистическая характеристика мошенничества в сети Интернет, противоправная деятельность интернет-мошенников а также особенности методики расследования указанного вида преступления.

Предметом исследования являются закономерности формирования общей методики расследования, а также использования специальных познаний в сфере высоких технологий и компьютерной информации при расследовании различных видов мошенничества с применением глобальной сети Интернет.

**Цели и задачи исследования.** Целью исследования является совершенствование общей методики расследования интернет-мошенничества, отвечающей современному уровню развития высоких информационных технологий, использования специальных познаний в сфере высоких технологий и компьютерной информации при расследовании преступлений данного вида, разработка научно обоснованных рекомендаций по организации взаимодействия следователя с экспертами и специалистами.

Для достижения указанной цели сформулированы следующие основные задачи:

1. Изучить и провести анализ научных концепций понятий «криминалистическая характеристика преступления», «специальные познания», «специальные знания», «оперативно-розыскное мероприятие», практическая реализация которых в значительной мере определяет содержание методики расследования преступлений.
2. Определить особенности проведения оперативно-розыскных мероприятий и следственных действий, представляющих наибольшую трудность для субъектов расследования интернет-мошенничества.
3. Изучить практику взаимодействия следователя с лицами, обладающими специальными познаниями, при расследовании мошенничества в сети Интернет, и разработать предложения по её совершенствованию.
4. Разработать комплекс организационных и практических мер, а также методические рекомендации, направленные на повышение эффективности расследования мошенничества и смежных с ним преступлений, совершаемых в сети Интернет.
5. Проанализировать практику назначения и проведения судебной экспертизы, при производстве которой применяются специальные познания в сфере компьютерной информации и высоких технологий.

**Теоретические и методологические основы исследования**. Методологической основой исследования является диалектическая теория познания, формальная логика, криминалистическая методология и общетеоретические концепции криминалистики. В диссертационном исследовании использованы общенаучные методы познания (анализ, синтез, статистический метод), а также методы других наук, в частности основы теории информационной безопасности.

Теоретическую основу работы составили труды учёных в области криминалистики, оперативно-розыскной деятельности и судебной экспертизы: Т.В. Аверьяновой, P.C. Белкина, А.Ф. Волынского,
В.А. Образцова, A.M. Зинина, Е.Р. Россинской, В.О. Захаровой,
A.A. Эйсмана, A.A. Эксархопуло, А.Ю. Шумилова, Н.Г. Шурухнова,
Н.П. Яблокова, А.Н. Лепёхина, А.А. Шаевича, О.В. Тушкановой и других.

Нормативной базой исследования послужили Конституция и законы Российской Федерации, действующее уголовное и уголовно-процессуальное законодательство, указы Президента и постановления Правительства РФ по вопросам укрепления законности, правопорядка и борьбы с преступностью, Доктрина информационной безопасности, ведомственные нормативные правовые акты МВД России и Минюста России, руководящие разъяснения Пленума Верховного суда Российской Федерации.

Научная обоснованность и достоверность результатов исследования, выводов и рекомендаций обеспечивается реализацией апробированной методами научных исследований, анализом достаточно объёмного и содержательного теоретического и практического материала.

**Эмпирической базой исследования** послужили статистические данные МВД России, отчёты районных судов города Москвы, а также обзоры практики судебной коллегии по уголовным делам Верховного Суда Российской Федерации.

В процессе исследования использовались материалы включённого наблюдения за лицами, обладающими специальными познаниями, достаточными для совершения преступлений в сфере высоких технологий, а также материалы не систематизированных опросов специалистов в сфере информационных технологий.

Диссертантом использован также собственный опыт работы с техническими средствами и компьютерными сетями.

**Научная новизна исследования** обусловлена тем, что оно является одним из первых специальных монографических исследований, посвящённых методике расследования мошенничества в сети Интернет, особенностям проведения оперативно-розыскных мероприятий и следственных действий, использования специальных познаний в области компьютерной техники и высоких информационных технологий, а также в уточнении существующих и создании новых теоретических и практических рекомендаций по расследованию указанных преступлений. Например, исследованы тактические особенности допроса обвиняемого и подозреваемого в совершении мошенничества в сети Интернет, результатом чего стал примерный список вопросов, ответы на которые помогут следователю качественно и количественно повысить информативность данного следственного действия. Также при исследовании непроцессуальных форм применения специальных познаний сделан вывод о необходимости совершенствования механизма взаимодействия правоохранительных органов и служб информационной безопасности организации, пострадавшей от действий интернет мошенников. В частности, материалы ведомственного расследования, проведённого внутри организации, должны помочь следователю в проведении таких следственных действий, как допрос, обыск и др.

На основе изученного теоретического и практического материала системно проанализированы правовые, процессуальные, организационные и методические аспекты методики расследования интернет-мошенничества по уголовному законодательству Российской федерации.

Новизна данного исследования нашла отражение в положениях, выносимых на защиту.

**Основные положения, выносимые на защиту.**

1. Авторское определение обстановки совершения интернет-мошенничества, под которой понимается система взаимообусловленных и взаимосвязанных элементов, в пространственных и временных границах которых происходит взаимодействие между преступниками и их жертвами, а также тех обстоятельств объективной среды, которые имели место на момент расследования и оказывали влияние на формирование следов преступления, его выявление и расследование.
2. Авторское определение специальных познаний с точки зрения практики расследования мошенничества в сети Интернет – это углублённые систематизированные знания в области высоких информационных технологий и компьютерной техники, доступные относительно узкому кругу профессионалов, а также практические навыки использования этих знаний, выработанные в процессе профессиональной деятельности.
3. Рекомендации по организации взаимодействия следователя со сведущими лицами при производстве оперативно-розыскных мероприятий и следственных действий при расследовании преступлений, связанных с использованием средств компьютерной техники.
4. Конкретные рекомендации по производству некоторых следственных действий, в частности, обыска, допроса подозреваемого и потерпевшего.
5. Выделены и систематизированы виды и особенности использования специальных познаний в области компьютерной информации и высоких технологий на различных стадиях раскрытия и расследования интернет-мошенничества.
6. Классификация вопросов, которые, в зависимости от сложившейся ситуации, целесообразно ставить перед экспертом при назначении компьютерно-технической экспертизы при расследовании интернет-мошенничества.

**Теоретическая и практическая значимость исследования**. Теоретическая значимость исследования определяется вкладом диссертанта в развитие теоретических и практических аспектов разработки и реализации методики расследования мошенничества в сети Интернет. Содержащиеся в работе положения и выводы направлены на углубление, обобщение и конкретизацию организационных и тактических особенностей по указанным уголовным делам. Они могут быть полезными для дальнейших исследований, связанных с проблемами расследования корыстных преступлений, совершаемых в сети Интернет путём обмана и злоупотребления доверием, а также других преступлений в сфере высоких информационных технологий.

Практическая значимость исследования состоит в том, что разработанные в диссертации научные положения и практические рекомендации призваны способствовать повышению эффективности правоприменительной деятельности органов предварительного расследования.

Предложения и рекомендации, сформулированные по результатам проведённого исследования, могут применяться в преподавании в высших учебных заведениях, а также при подготовке или повышении квалификации работников правоохранительных органов, специализирующихся, в частности, на расследовании интернет-мошенничества и других преступлений, совершаемых в глобальной сети.

**Апробация результатов исследования**. Сформированные в диссертации теоретические положения, выводы, предложения и практические рекомендации отражены в четырёх опубликованных работах диссертанта, в том числе в двух, опубликованных в ведущих рецензируемых научных журналах и изданиях, утверждённых ВАК Минобрнауки России.

Также результаты диссертации внедрены и используются в учебном процессе кафедрой документационного обеспечения управления и прикладной лингвистики Российского государственного технологического университета имени К.Э. Циолковского при подготовке студентов по дисциплине «Информационная безопасность и защита информации».

**Структура диссертации**. Объём и структура диссертации определены предметом исследования, его целями, задачами и результатами. Работа состоит из введения, трёх глав, включающих в себя двенадцать параграфов, заключения и списка использованной литературы.

**Содержание работы**

Во **введении** обоснована актуальность и научная новизна темы, определены степень её разработанности, предмет, цели и задачи исследования, изложены теоретические и методологические основы исследования, сформулированы положения, выносимые на защиту, отражена значимость результатов диссертационного исследования и его структура.

Первая глава диссертации **«Обстоятельства, подлежащие установлению при расследовании мошенничества в сети Интернет»** состоит из пяти параграфов.

Первый параграф *«Общая характеристика мошенничества: криминалистический аспект»* посвящён криминалистической характеристике мошенничества в целом, и особенно, мошенничества в сети Интернет. В частности, на основе изученных подходов к решению вопроса о содержании понятия криминалистической характеристики мошенничества, выделены пять основных элементов, которые были взяты за основу для дальнейшего раскрытия криминалистической характеристики интернет-мошенничества.

В результате проведённого в параграфе анализа криминалистической характеристики интернет-мошенничества автором сделан ряд выводов. В частности, для определения понятия мошенничества предлагается использовать не только термин «хищение», но и «завладение». Обман и злоупотребление доверием как способы мошенничества подразумевают достижение определённых промежуточных результатов перед окончательным получением чужого имущества или получением права на него, а именно введение в заблуждение собственника или владельца имущества таким образом, чтобы преступник впоследствии именно получил имущество от жертвы.

Также автором обосновывается вывод о том, что мошенничество в сети Интернет, в силу своих особенностей, посягает не конкретно на имущество, а на право на это имущество. Поскольку УК РФ не содержит подробной информации о том, что необходимо понимать под правом на имущество в контексте его (кодекса) статей, то может возникнуть вопрос о том, считать ли преступление оконченным с момента получения полного права собственности на имущество, или же речь идёт только о каком-то определённом правомочии (владения, пользования или распоряжения).

Данный вопрос автор предлагает решать в каждом конкретном случае. Так как права на имущество (а также объём этих прав) закрепляются в соответствующих документах, то в случаях, когда предметом посягательства при совершении интернет-мошенничества является право на чужое имущество, преступление должно считаться оконченным с того момента, когда преступник наделяется тем объёмом прав, которым, на основании соответствующих документов, была наделена жертва, либо, в том объёме, в каком это необходимо для производства действий с имуществом.

Во втором параграфе *«Обстановка совершения преступления»* рассматриваются различные подходы к пониманию данного термина как одного из элементов криминалистической характеристики интернет-мошенничества.

В результате анализа позиций различных учёных, автором предложено собственное определение обстановки совершения преступления с точки зрения исследования мошенничества в сети Интернет –это *система взаимообусловленных и взаимосвязанных элементов, в пространственных и временных границах которых происходит взаимодействие между преступниками и их жертвами, а также тех обстоятельств объективной среды, которые имели место на момент расследования и оказывали влияние на формирование следов преступления, его выявление и расследование*.

В третьем параграфе *«Способ совершения преступления»* исследуются основные виды мошенничества в сети Интернет и предлагаются критерии для их классификации. Все виды мошенничества в сети Интернет можно условно объединить в следующие группы:

1. основанные преимущественно на использовании электронной почты и/или иных средств обмена сообщениями как основных инструментов воздействия на жертву;
2. мошенничества, в схемах которых центральное место отводится применению сайтов.

В параграфе дана характеристика массовой рассылки специальных сообщений (спама) как одного из инструментов воздействия со стороны интернет-мошенника на потенциальную жертву, а также параметры, которым должны соответствовать эти сообщения. Кроме того, описаны конкретные виды интернет-мошенничества, в которых применяется метод рассылки спама: нигерийские письма и мошенничество в социальных сетях.

При рассмотрении мошенничеств, в которых посягательство на объект осуществляется преимущественно с использованием возможностей интернет-сайтов автором предложен список основных направлений деятельности мошенников:

1. инвестиционные схемы;
2. заработок;
3. «волшебные кошельки»;
4. аукционы и интернет-торговля;
5. кардинг;
6. онлайн-казино и лотереи;
7. клонирование сайтов.

Кроме того, дана характеристика каждого из указанных направлений.

В конце параграфа высказывается и обосновывается точка зрения, согласно которой в скором времени большое распространение получит так называемое мошенничество в онлайн-играх.

В последние 3-5 лет всё большую популярность приобретают mmo-игры (массовые многопользовательские онлайн-игры), в которых тысячи пользователей сети Интернет имеют возможность совместно проводить досуг. За эти годы аудитория данного вида развлечений существенно возросла, как и количество представленных разработчиками игр. В связи с этим также существенно возросла активность мошенников и разработчиков вредоносного программного обеспечения. Учитывая крайне слабую разработанность данной проблематики в российской науке, а также вопросов взаимодействия реальной и виртуальных экономик в целом, представляется возможным заключить, что правоприменительные органы могут столкнуться с нехваткой знаний для качественного проведения предварительного расследования по этому виду интернет-мошенничества.

В четвёртом параграфе *«Общая характеристика типичного преступника»* рассмотрена личность интернет-мошенника с точки зрения криминологии и криминалистики.

В работе отмечается, что, несмотря на то, что соотношение мужчин и женщин среди пользователей сети Интернет примерно одинаково, тем не менее, интернет-мошенниками чаще всего становятся мужчины.

При анализе возраста типичного интернет-мошенника отмечается низкий средний возраст преступников, что свидетельствует о постепенном омоложении части преступности вообще.

Одной из характерных особенностей интернет-преступности вообще и интернет-мошенничества, в частности, является отсутствие судимости у преступников. Если сравнивать мошенничество в сети Интернет и обычное мошенничество, то можно увидеть, по сути, две противоположные картины. По сравнению с традиционными видами мошенничества интернет-мошенничество является достаточно молодым видом преступления.

В конце параграфа, анализируя качества личности преступника, автором высказано мнение о том, что в некоторых случаях одним из важных качеств личности интернет-мошенника является наличие организаторских способностей, поскольку некоторые виды интернет-мошенничества являются технически сложными в плане исполнения, поэтому в их совершении могут принимать участие несколько человек.

В пятом параграфе *«Общая характеристика круга потерпевших»* автором разделены на подгруппы и охарактеризованы лица, способные быть потерпевшими от мошенничества в сети Интернет. Учитывая то, что интернет-мошенничество носит корыстный характер, автор считает возможным выделить следующие подгруппы потерпевших:

1. физические лица, в том числе иностранные;
2. предприятия связи и провайдеры сети Интернет;
3. банки и другие кредитные организации;
4. магазины электронной торговли;
5. другие коммерческие и некоммерческие организации;
6. другие иностранные юридические лица.

В независимости от того, о каком виде мошенничества в Интернете идёт речь, характеристика круга потерпевших лиц, во многом, похожа. Большинство жертв интернет-мошенников являются людьми, слабо знакомыми с техникой безопасности при работе в Сети.

Потерпевшего также характеризует само преступление, жертвой которого он стал. В зависимости от того, в какой области действовал мошенник, его жертвам могут быть присущи такие характеристики как: склонность к азартным играм (мошенничества с фальшивыми онлайн-казино), опрометчивость, самонадеянность, желание лёгкой наживы (мошенничества с инвестиционными схемами и платёжными системами) и др.

Вторая глава диссертации **«Особенности производства первоначальных следственных действий и оперативно-розыскных мероприятий»** состоит из трёх параграфов.

В первом параграфе *«Особенности проведения некоторых оперативно-розыскных мероприятий»* рассмотрены общие вопросы организации оперативно-розыскной деятельности при расследовании мошенничества в сети Интернет.

Кроме того, рассмотрены вопросы проведения некоторых оперативно-розыскных мероприятий, которые представляются наиболее важными при расследовании интернет-мошенничества.

Исследование указанных вопросов позволило автору диссертации сделать следующие выводы:

1. Учитывая специфику преступности в сети Интернет оперативно-розыскные мероприятия можно классифицировать по следующим основаниям:

1. Законодательная классификация:
	1. опрос;
	2. наведение справок;
	3. сбор образцов для сравнительного исследования;
	4. проверочная закупка;
	5. исследование предметов и документов;
	6. наблюдение;
	7. отождествление личности;
	8. обследование помещений, зданий, сооружений, участков местности и транспортных средств;
	9. контроль почтовых отправлений, телеграфных и иных сообщений;
	10. прослушивание телефонных переговоров;
	11. снятие информации с технических каналов связи;
	12. оперативное внедрение;
	13. контролируемая поставка;
	14. оперативный эксперимент.
2. В зависимости от ограничения прав и свобод граждан:
	1. ОРМ, не ограничивающие конституционные права граждан (опрос, наблюдение, наведение справок, сбор образцов для сравнительного исследования (в том числе и компьютерных программ), проверочная закупка, исследование предметов и документов, отождествление личности, оперативное внедрение, контролируемая поставка и оперативный эксперимент);
	2. ОРМ, ограничивающие конституционные права граждан (негласное обследование помещений, зданий, сооружений, участков местности и транспортных средств, контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи).
3. В зависимости от продолжительности проведения:
	1. разовые ОРМ (опрос, наведение справок, отождествление личности, оперативный эксперимент, закупка и т.д.);
	2. длящиеся ОРМ (контроль почтовых отправлений, оперативное внедрение, прослушивание телефонных переговоров, наблюдение и т.д.).
4. В зависимости от видов санкционирования:
	1. не требующие какого-либо санкционирования:
		1. опрос;
		2. наведение справок;
		3. сбор образцов для сравнительного исследования;
		4. исследование предметов и документов;
		5. наблюдение;
		6. отождествление личности;
		7. проверочная закупка и контролируемая поставка предметов, свободная реализация которых разрешена.
	2. требующие ведомственного санкционирования руководителем органа, осуществляющего ОРД:
		1. проверочная закупка и контролируемая поставка предметов, свободная реализация которых разрешена;
		2. оперативный эксперимент;
		3. оперативное внедрение.
	3. требующие судебного санкционирования:
		1. контроль почтовых отправлений, телеграфных и иных сообщений;
		2. прослушивание телефонных переговоров;
		3. снятие информации с технических каналов связи;
		4. негласное обследование помещений, зданий, сооружений, участков местности и транспортных средств.

2. Оперативно-розыскное мероприятие – составная часть оперативно-розыскной деятельности, сведения об организации и тактике которой составляют государственную тайну, представляющую собой совокупность действий специально уполномоченных на то государственных органов и их должностных лиц, осуществляемых с соблюдением регламентированных законом оснований и условий, отвечающую нормам морали и нравственности и непосредственно направленную на достижение целей и разрешение задач оперативно-розыскной деятельности.

3. Снятие информации с технических каналов связи (с точки зрения расследования мошенничества в сети Интернет) – это регламентированное законом об ОРД оперативно-розыскное мероприятие, проводимое на основании судебного решения, заключающееся в негласном съёме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путём контроля специальными техническими средствами и программным обеспечением работы соответствующих систем и устройств, а также излучаемых ими электромагнитных и других полей.

4. В тех случаях, когда используемый подозреваемыми в интернет-мошенничестве способ связи совмещён с обычной и/или мобильной телефонной связью, необходимо говорить не только о снятии информации с технических каналов связи, но и о прослушивание телефонных переговоров. В таких ситуациях необходимо учитывать требования, предъявляемые не только к снятию информации с технических каналов связи, но и к прослушиванию телефонных переговоров.

5. С точки зрения интернет-мошенничества различают физическое, электронное и комплексное наблюдение. Комплексное наблюдение позволяет получить больше информации о наблюдаемом лице, чем физическое и электронное по отдельности. Однако залогом успешности использования такого наблюдения является эффективное применение специальных знаний специалиста и специальных приборов.

Во втором параграфе *«Тактические особенности допроса обвиняемого»* анализируются особенности проведения допроса подозреваемого и обвиняемого при расследовании мошенничества в сети Интернет.

В процессе исследования указанной проблематики автором предложен список вопросов, которые целесообразно задать обвиняемому в интернет-мошенничестве при проведении допроса. Особенностью этого списка является то, что, с одной стороны, составляющие его вопросы являются общими и могут использоваться при расследовании практически любых интернет-мошенничеств, а с другой – являются специальными, поскольку некоторые из них не применимы к расследованию, например, традиционных видов мошенничества. Для удобства восприятия, в зависимости от цели, которую преследует следователь, предложенные вопросы объединены в три категории:

1. вопросы, направленные на установление и конкретизацию ущерба;
2. вопросы, направленные на установление конкретного способа совершения интернет-мошенничества и сокрытия следов преступления;
3. вопросы, направленные на получение информации о личности подозреваемого/обвиняемого, а также о возможных соучастниках.

Кроме того, рассмотрены приёмы преодоления противодействия со стороны обвиняемого в интернет-мошенничестве. Поскольку мошенники обладают «живым» умом, то если они решили противодействовать следствию, основным оружием следователя должен стать интеллект, конечной целью применения которого должно стать уличение допрашиваемого во лжи, постановка перед необходимостью сотрудничать со следствием.

В конце параграфа делается вывод о том, что специфика работы следователя обязывает его находить общий язык со всеми лицами, с которыми приходится контактировать. В этой связи очень важной задачей является создание прочных личных и деловых связей с широким кругом специалистов. В частности, при подготовке к допросу обвиняемого, как и потерпевшего, в интернет-мошенничестве, при наличии реальной возможности, следователю рекомендуется проконсультироваться с психологом для построения наиболее эффективной тактики допроса.

В третьем параграфе раскрываются основные тактические особенности допроса потерпевшего от мошенничества в сети Интернет. Отмечается, что, как и в случае с допросом обвиняемого, общие вопросы пострадавшему можно объединить в три группы. Основным назначением предложенных в параграфе вопросов является построение следователем наиболее эффективной тактики допроса потерпевшего, в котором следователь сможет получить максимум криминалистически значимой информации.

Также, в процессе рассмотрения особенностей проведения допроса, отмечается склонность некоторых потерпевших от интернет-мошенничества скрывать не только отдельные факты, свидетельствующие о совершённом деянии, но и вообще скрывать свой статус. В этой связи приводятся примеры тактических приёмов, направленных на преодоление такого противодействия.

В конце параграфа автор акцентирует внимание на необходимости учёта положения допрашиваемого лица. Например, если он является служащим банка, а уголовное дело возбуждено по факту мошенничества с кредитными картами, то вполне возможно, что сведения, которые он скрывает, могут быть связаны с банковской тайной. В связи с этим рекомендуется более тщательно подходить к подготовке и проведению допроса. Полезным будет подробно разъяснить, что информация, полученная на допросе, не будет передана посторонним лицам.

В четвёртом параграфе анализируются особенности тактики проведения обыска как одного из наиболее сложных следственных действий, наравне с допросом обвиняемого и подозреваемого.

С учётом положений уголовно-процессуального законодательства Российской Федерации и особенностей совершения мошенничества в сети Интернет, автор указывает объекты поиска, среди которых:

а) орудия совершения преступления или их составные части (компьютеры и другие электронные устройства, а также детали от них и др.);

б) предметы со следами совершённого преступления;

в) предметы–результаты преступной деятельности (поддельные документы, фальшивые деньги и т.д.);

г) похищенное имущество, документы, деньги или ценности;

д) скрывшийся мошенник;

е) документы, отражающие важные для дела обстоятельства (записные книжки, квитанции, чеки и т.д.);

ж) образцы для сравнительного исследования (в том числе образцы программ, образцы текстов, хранящихся на компьютере обыскиваемого и т.д.) и др.;

Анализируя участие понятых в работе указывается на необходимость для следователя заранее предусмотреть, чтобы приглашённые понятые имели определённые познания в области информационных технологий. При проведении следственных действий по делам об интернет-мошенничестве и других компьютерных преступлениях эта рекомендация является необходимой.

В ходе характеристики тактики обыска на подготовительной, обзорной и детальной стадиях автор предлагает рекомендации. Например, на обзорной стадии следователю рекомендуется, обращать внимание на компьютеры в обыскиваемом помещении и пространство вокруг них: наличие периферических подключенных устройств, иные предметы рядом с компьютерами (например, накопители памяти различных форматов). Также следует обратить внимание на провода, подсоединённые к компьютеру, а точнее, куда они идут. Вполне возможно, что к компьютеру, принадлежащему подозреваемому в интернет-мошенничестве, подключён спрятанный накопитель, где хранятся данные, представляющие ценность для расследования факта интернет-мошенничества.

Кроме того, автором акцентируется внимание на то, что в ходе проведения обыска, особенно в детальной стадии, следователю желательно постоянно взаимодействовать со специалистом, который осуществляет помощь в обнаружении следов преступления, связанных с использованием компьютеров, а также консультирует членов оперативно-розыскной группы по вопросам, связанным и информационными технологиями, имеющим отношение к уголовному делу.

Третья глава **«Использование специальных познаний при расследовании мошенничества в сети Интернет»** посвящена особенностям использования помощи сведущих лиц при расследовании интернет-мошенничества и состоит из двух параграфов.

В первом параграфе *«Процессуальные формы использования специальных познаний»* обосновывается необходимость применения специальных познаний при расследовании мошенничества в сети Интернет, а также классификация форм использования этих познаний при проведении предварительного расследования. В частности, автором выделены следующие основные формы:

1. Процессуальные формы использования специальных познаний:
	1. участие специалиста в производстве следственных действий;
	2. участие специалиста в судебном разбирательстве;
	3. производство судебной экспертизы и дача заключения специалиста, а также показания эксперта и показания специалиста.
2. Непроцессуальные формы использования специальных познаний:
	1. оказание сведущими лицами (специалистами и экспертами) справочно-консультативной помощи сотрудникам правоохранительных органов;
	2. участия специалистов в оперативно-розыскных мероприятиях;
	3. выполнения ревизионных и аудиторских проверок;
	4. проведение специалистом предварительных исследований материальной обстановки места происшествия и вещественных доказательств во время его участия в следственных действиях.

В ходе анализа некоторых терминов автором обосновывается приоритет использования термина «познание» перед «знанием». Знания представляют собой существующую, готовую к усвоению субъектом информацию. Лицо, усвоившее большое количество знаний в одной или нескольких областях, может считаться не специалистом. Познание же включает такой важный элемент, как понимание знаний, позволяющее применять усвоенные знания на практике. Термин «познание» подразумевает процессуальность, что, на наш взгляд, является основой работы специалиста и эксперта.

Также, рассматривая вопрос о том, какие познания можно считать специальными, автором предложено определение специальных познаний с точки зрения мошенничества в сети Интернет *– это углублённые систематизированные знания высоких информационных технологий и компьютерной техники, доступные относительно узкому кругу профессионалов, а также практические навыки использования этих знаний, выработанные в процессе профессиональной деятельности.*

При рассмотрении вопросов участия специалиста в следственных действиях отмечается, что при подготовке к следственному действию, а также назначая судебную экспертизу, необходимо учитывать предметную специализацию эксперта и специалиста, на что также обращают внимание и некоторые другие учёные.

В параграфе указывается, что при расследовании мошенничества в сети Интернет основной экспертизой является компьютерно-техническая. Кроме того, даётся краткая историческая справка о формировании данного рода экспертиз.

При производстве компьютерно-технической экспертизы компьютера либо иного устройства подозреваемого либо обвиняемого в совершении интернет-мошенничества, в зависимости от конкретного вида компьютерно-технической экспертизы, производится исследование следующих объектов:

1. Аппаратные объекты:
	1. компьютеры;
	2. комплектующие для компьютеров и других устройств;
	3. периферические устройства (принтеры, сканеры, модемы и т.д.);
	4. сетевые аппаратные средства (серверы, сетевые кабели и т.д.);
	5. интегрированные системы (мобильные телефоны, органайзеры и др.).
2. Программные объекты:
	1. системное программное обеспечение;
	2. прикладное программное обеспечение.
3. Информационное объекты (данные):
	1. документы, изготовленные с помощью компьютерных средств;
	2. данные в мультимедийные форматах (аудио- и видеофайлы, изображения и т.д.);
	3. компьютерная информация, содержащаяся в базах данных.

На основе представленной классификации объектов, а также собственного опыта изучения работы компьютеров и других электронных устройств, автором предложены вопросы, которые целесообразно поставить на разрешение перед экспертом при назначении компьютерно-технической экспертизы.

В процессе разбирательства дела о мошенничестве в суде специалист может предоставить следующую информацию:

1. об оперативно-розыскных мероприятиях и следственных действиях, в которых он участвовал;
2. сведения справочно-информационного характера;
3. проконсультировать по общим и частным вопросам с целью правильного понимания судом и другими участниками судебного заседания всех материалов уголовного дела об интернет-мошенничестве.

Некоторые исследователи выделяют применение следователем специальных познаний как одну из форм использования специальных познаний.

Собственные познания следователя в области высоких технологий в большинстве случаев могут оказаться недостаточными для самостоятельного исследования компьютерной техники. Даже если следователь обладает необходимыми специальными знаниями, что может быть обусловлено его предыдущей профессией, наличием соответствующего диплома, сертификатов и т.п., необходимо привлечение эксперта или специалиста для дачи заключения.

Во втором параграфе *«Непроцессуальные формы использования специальных познаний»* раскрыты вопросы применения форм использования помощи сведущих лиц, не регламентированных (форм) УПК РФ. Автор выделяет 6 основных непроцессуальных функций:

1. консультации следователя по вопросам, требующим специальных познаний;
2. составление различных справок по поручению следователя (справочная деятельность сведущего лица);
3. использование результатов внесудебных (ведомственных, административных) исследований (расследований), проводимых специальными комиссиями;
4. оказание технической помощи следователю (например, помощь в установке отслеживающего программного обеспечения на компьютер подозреваемого в интернет-мошенничестве);
5. использование результатов проверок, проводимых работниками различных ведомств и инспекций;
6. использование материалов предварительного (внесудебного) экспертного исследования различных объектов (например, вещественных доказательств).

Приведённые выше функции автор объединяет в три основные формы непроцессуального использования специальных познаний, применимых в расследовании интернет-мошенничества: участие специалиста в оперативно-розыскных мероприятиях, оказание справочно-информационной помощи следователю и консультационная деятельность.

Особое внимание автор уделяет использованию результатов ведомственного расследования (в случаях, потерпевшим от действий интернет-мошенника является юридическое лицо) как одному из самых ценных источников криминалистически значимой информации.

Результаты ведомственного расследования факта интернет-мошенничества могут использоваться следователем при проведении следственных действий и назначении судебных экспертиз. В частности, такая информация позволит: во-первых, формулировать более конкретные вопросы и задания эксперту при подготовке постановления о назначении экспертизы; во-вторых, более ясно представлять себе общую картину преступления, с меньшими трудностями подбирать специалистов для каждого следственного действия; в-третьих, выявить и разыскать сообщников интернет-мошенника, если они были.

В **заключении** диссертации содержатся основные выводы и предложения, полученные в ходе диссертационного исследования.

**Положения диссертационного исследования отражены в следующих публикациях автора:**

**Работы, опубликованные в ведущих рецензируемых научных журналах и изданиях, утверждённых ВАК Минобрнауки России**

1. Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные проблемы российского права. – 2010. – № 4 (17). – 0,29 п.л.
2. Атаманов Р.С. Криминалистическая характеристика мошенничества в онлайн-играх // Российский следователь. – 2011. – № 21. – 0,26 п.л.

**Научные статьи, опубликованные в иных изданиях**

1. Атаманов Р.С. Правонарушения, совершаемые в сети Интернет, связанные с обманом и злоупотреблением доверием с целью получения конфиденциальной информации: некоторые проблемы и способы их решения // Правовые вопросы связи. – № 2. – 2010. – 0,3 п.л.
2. Атаманов Р.С., Волохова О.В. Интернет-мошенничество в социальных сетях // Система отправления правосудия по уголовным делам в современной России как социальное взаимодействие личности и государства: сборник научных статей: в 2 ч. Ч. 1. – Курск, 2009. – 0,16 п.л.
1. Данные официальной статистики МВД о состоянии преступности / <http://www.mvd.ru/presscenter/statistics/reports/> (последнее обращение – 14.05.2012). [↑](#footnote-ref-1)