На правах рукописи

КОСЫНКИН Александр Александрович

ПРЕОДОЛЕНИЕ ПРОТИВОДЕЙСТВИЯ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

12.00.09 – уголовный процесс, криминалистика;
оперативно-розыскная деятельность

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
кандидата юридических наук

Саратов – 2012

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Мордовский государственный университет им. Н.П. Огарёва»

Научный руководитель - доктор юридических наук, доцент
Подольный Николай Александрович

Официальные оппоненты: доктор юридических наук, профессор
Макаренко Илона Анатольевна

кандидат юридических наук, доцент
Анненков Сергей Иванович

Ведущая организация - ФГБОУ ВПО **«Юго-Западный государственный университет»**
(юридический факультет)

Защита состоится 28 марта 2012 г. в 15:00 часов на заседании диссертационного совета Д-212.239.01 при Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Саратовская государственная юридическая академия» по адресу: 410056, г. Саратов, ул. Чернышевского, 104, ауд. 102.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Саратовская государственная юридическая академия».

Автореферат разослан «____» февраля 2012 г.

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент **Е.В. Кобзева**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Бурное развитие высоких технологий обеспечивает общество наряду с комфортом жизнедеятельности каждого его члена также проблемами, связанными с появлением и развитием новых видов преступности. Одним из таких видов является преступность в сфере компьютерной информации, образуемая деяниями, предусмотренными ст. ст. 272-274 Уголовного кодекса Российской Федерации.

Согласно данным официальной статистики МВД России, в настоящее время наблюдается серьезное сокращение числа преступлений, совершаемых в сфере компьютерной информации. Так, если в 2009 г. их было зарегистрировано 11636, то в 2010 г. – 7398. При этом в 2010 г. сокращение зарегистрированных преступлений названного вида составило 36,4%, а за 11 месяцев 2011 г. – 63,9%[1]. Вполне понятно, что приведенные показатели свидетельствуют не об уменьшении случаев совершения компьютерных преступлений, а о высокой латентности последних, о том, что выявлять их стало гораздо сложнее. Тем более что ещё в 2009 г. фиксировалось увеличение числа зарегистрированных преступлений в сфере компьютерной информации на 29,1%.

Одной из причин сложившегося положения дел служит совершенствование противодействия проводимому расследованию данного вида преступлений со стороны как виновных лиц, так и иных заинтересованных в сокрытии истины субъектов. На эффективность оказываемого расследованию противодействия указывает и падение раскрываемости преступлений в сфере компьютерной информации. Так, в 2010 г. раскрываемость данного вида преступлений уменьшилась на 39,8%, а за 11 месяцев 2011 г. – на 61,2%. Причём с января по декабрь 2009 г. наблюдался рост раскрываемости на 34,2%[2].

Таким образом, очевидно, что государство постепенно уступает инициативу в пользу криминализированных сообществ и индивидуально действующих лиц, не признающих каких-либо ограничений в сфере компьютерной информации. Между тем, это абсолютно недопустимо, поскольку компьютерные и иные высокие технологии становятся неотъемлемым компонентом механизма управления государством и обществом.

Одним из частных средств борьбы, в которой государство должно проявлять себя как поборник порядка в сфере компьютерной информации, является умелая организация расследования каждого конкретного преступления, совершенного в данной сфере. В связи с этим особенно острой становится необходимость формирования научно обоснованного подхода к

---

[1] См. : Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения — 17.01.2012).

[2] См. : Там же.

определению системы действий и мероприятий по преодолению противодействия расследованию преступлений в сфере компьютерной информации. В свою очередь, разработка таких мер возможна лишь на основе исследования самого противодействия, которое оказывается проводимому расследованию. Необходимо выявление «слабых» сторон этого противодействия с тем, чтобы действия правоохранительных органов по его преодолению были успешны и обеспечивали качественное расследование совершённых преступлений. Сложность действий по оказанию противодействия расследованию преступлений в сфере компьютерной информации требует исследования, посвящённого только им.

Степень научной разработанности проблемы.

Вопросы методики и тактики расследования преступлений в сфере компьютерной информации рассматривались в трудах таких ученых, как Т.В. Аверьянова, Б.В. Андреев, А.В. Варданян, В.Б. Вехов, Ю.В. Гаврилин, М.В. Гаврилов, А.Ю. Головин, А.С. Егорышев, А.Н. Иванов, Д.А. Илюшин, В.В. Крылов, В.А. Мещеряков, Е.В. Никитина, П.Н. Пак, Н.А. Подольный, В.В. Попова, В.Ю. Рогозин, Е.Р. Россинская, А.В. Рыбин, Л.Н. Соловьев, А.Ю. Усов, В.П. Хорст, Н.Г. Шарухнов.

Проблемам расследования преступлений в сфере компьютерной информации посвящены диссертационные исследования В.Ю. Рогозина (1998), А.В. Остроушко (2000), Ю.В. Гаврилина (2000), В.А. Мещерякова (2001), У.А. Мусаевой (2002), С.В. Крыгина (2002), В.П. Хомколова (2004), А.С. Егорышева (2004), Р.А. Белевского (2006).

Большое значение для решения проблем преодоления противодействия расследованию преступлений в сфере компьютерной информации имеют работы, в которых исследовались вопросы уголовно-правовой и криминологической характеристики названных преступлений. В связи с этим следует отметить труды таких учёных, как Р.М. Айсанов, С.Д. Бражник, М.Ю. Дворецкий, А.М. Доронин, К.Н. Евдокимов, У.В. Зинина, М.А. Зубова, И.А. Сало, Т.Г. Смирнова, М.В. Старичков, В.Г. Степанов-Егиянц, С.С. Шахрай, Д.А. Ястребов.

Общие проблемы противодействия расследованию преступлений и его преодоления исследовались Э.У. Бабаевой, С.Т. Гогаевым, А.Ю. Головиным, Л.Я. Драпкиным, В.Н. Карагодиным, А.М. Кустовым, В.П. Лавровым, Р.Г. Мартыненко, Р.Ш. Осипяном, Н.А. Подольным. Также они были и предметом диссертационных исследований С.Ю. Журавлева (1992), В.Н. Карагодина (1992), Л.В. Лившица (1998), О.Л. Стулина (1999), А.Н. Петровой (2000), М.В. Щеголевой (2001), И.В. Нецкина (2001), А.Ю. Федоренко (2001), А.Е. Маслова (2001), Е.В. Варфоломеева (2002), А.И. Звягина (2004), И.И. Фуражкиной (2004), Р.Г. Мартыненко (2004), А.А. Бибикова (2005), А.Б. Петруниной (2006).

Однако, несмотря на обилие работ, которые посвящены различным аспектам преступлений в сфере компьютерной информации, вопросы противодействия расследованию преступлений в сфере компьютерной

информации и его преодоления ранее в науке на монографическом уровне не исследовались.

Совокупностью указанных обстоятельств и обусловливается актуальность темы диссертационного исследования.

Объектом диссертационного исследования являются общественные отношения, связанные с расследованием преступлений в сфере компьютерной информации, предусмотренных главой 28 УК РФ.

Предмет диссертационного исследования образуют нормы Конституции РФ, уголовного и уголовно-процессуального законодательства России, иных нормативно-правовых актов, регулирующие отношения, связанные с расследованием преступлений в сфере компьютерной информации, а также материалы следственной и судебной практики в части установления признаков противодействия расследованию преступлений в сфере компьютерной информации и его преодоления.

Цель и задачи диссертационного исследования. Целью исследования является формирование концепции информационного подхода к разработке системы действий и мероприятий по преодолению противодействия расследованию преступлений в сфере компьютерной информации.

Для разрешения названной цели были поставлены и решены следующие задачи:

1) определить место противодействия среди иных видов препятствий проводимому расследованию преступлений, в том числе совершаемых в сфере компьютерной информации;

2) установить природу и механизм противодействия расследованию преступлений в сфере компьютерной информации;

3) выявить основные формы противодействия расследованию преступлений в сфере компьютерной информации;

4) определить структуру противодействия расследованию преступлений в сфере компьютерной информации и установить значение отдельных ее элементов для организации и проведения действий и мероприятий по преодолению такого противодействия;

5) очертить круг субъектов противодействия расследованию преступлений в сфере компьютерной информации;

6) выявить способы противодействия расследованию преступлений в сфере компьютерной информации;

7) установить особенности преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии возбуждения уголовного дела;

8) разработать тактические приёмы, тактические операции и тактические комбинации, подлежащие применению в рамках организации и проведения действий и мероприятий по преодолению противодействия расследованию преступлений в сфере компьютерной информации.

Методологическую основу исследования составил диалектико-материалистический метод познания и основанные на нем общенаучные и специальные методы. В работе использованы системно-структурный, логико-

юридический, конкретно-социологический (анкетирование), сравнительно-исторический, сравнительно-правовой методы, а также общепринятые методики исследования документов, периодических изданий, статистических данных.

Нормативной базой диссертации стали Конституция Российской Федерации, уголовное и уголовно-процессуальное законодательство, законодательство об оперативно-розыскной деятельности.

Теоретическую основу проведенного **исследования** составили, главным образом, труды известных ученых-криминалистов, таких как Т. В. Аверьянова, Р. С. Белкин, Н. Т. Ведерников, И. А. Возгрин, Т. С. Волчецкая, А. Ф. Волынский, Ю. П. Гармаев, Л. Я. Драпкин, Г. Г. Зуйков, М. К. Каминский, В. Н. Карагодин, В. Я. Колдин, В.И. Комисаров, А. М. Кустов, В. П. Лавров, А. Ф. Лубин, М. А. Лушечкина, И. А. Макаренко, В. М. Мешков, В. А. Образцов, Н.А. Подольный, А.С. Подшибякин, А. Р. Ратинов, Е. Р. Россинская, Н. А. Селиванов, В.В. Степанов, Л.Г. Шапиро, Н. Г. Шурухнов, Н. П. Яблоков, И. Н. Якимов и др.

Эмпирическая база диссертации включает:

– материалы 115 уголовных дел о преступлениях в сфере компьютерной информации, рассмотренных судами Республики Мордовия, Пензенской и Ульяновской областей за период с 1995 по 2011 гг., а именно протоколы следственных действий (допросов, очных ставок, осмотров мест происшествия), постановления о привлечении лица в качестве обвиняемого, приговоры;

– результаты анкетирования следователей прокуратуры (следственного комитета) и органов внутренних дел по Республике Мордовия (87 человек), проведенного на предмет установления их мнения по вопросам противодействия расследованию преступлений в сфере компьютерной информации и преодоления такого противодействия;

– данные уголовной статистики о регистрации и раскрытии преступлений в сфере компьютерной информации в Республике Мордовия и Российской Федерации в период с 1998 по ноябрь 2011гг.

Научная новизна диссертационной работы определяется ее целью и задачами и состоит в формировании концепции информационного подхода к разработке системы действий и мероприятий по преодолению противодействия расследованию преступлений в сфере компьютерной информации.

Основой этой концепции является предложенная в диссертационном исследовании структура противодействия расследованию названного вида преступлений. При этом особое внимание было уделено специфике проявления отдельных элементов данной структуры и определению их значения для организации и проведения действий по преодолению противодействия расследованию преступлений в сфере компьютерной информации. На данной информационной основе были сформулированы предложения и рекомендации по преодолению противодействия, которое оказывается расследованию преступлений в сфере компьютерной информации.

Результатами диссертационного исследования проблем преодоления противодействия расследованию преступлений в сфере компьютерной информации стали следующие наиболее существенные **положения, выносимые** нами **на публичную защиту:**

1. Препятствия, осложняющие расследование преступлений в сфере компьютерной информации, делятся на факторы объективного, субъективного и условно объективного характера. Объективные – это факторы, которые возникают и реализуются независимо от воли конкретных лиц (кем бы они ни были - следователем или преступником) в виду определённого стечения обстоятельств, являющегося результатом действия объективно существующих сил или законов. Субъективные – это препятствия, создаваемые лицами, которые совершили преступление либо которые в силу различных причин не хотят, чтобы данное преступление было раскрыто, а также ошибки следователя, ведущего расследование, и должностных лиц, содействующих этому расследованию. Условно объективные – это особенности носителей компьютерной информации, которые могут стать причиной ее уничтожения.

Знание различий между указанными видами препятствий предполагает правильный выбор действий, направленных на их преодоление.

2. Наиболее часто противодействие расследованию преступлений в сфере компьютерной информации осуществляется в следующих формах: сокрытие и инсценировка преступления; использование средств массовой информации для воздействия на лиц, ведущих расследование; непосредственное воздействие на следователя и иных лиц, от которых зависит ход проводимого расследования.

Указанные формы определяют особенности противодействия расследованию преступлений в сфере компьютерной информации, отличающие его от противодействия расследованию иных видов преступлений.

3. Структура противодействия расследованию преступлений включает в себя следующие элементы:

1) субъект, оказывающий противодействие расследованию;
2) цель и мотив оказания противодействия;
3) объект, на который направлено противодействия расследованию;
4) средства и способ противодействия оказываемого расследованию;
5) время, место, обстановка, в которых осуществляется противодействие расследованию;
6) ошибки, допущенные следователем или лицами, содействующими ему в расследовании;
7) деятельность третьих лиц или случайных факторов, которые могут быть использованы в ходе оказываемого противодействия.

Особенности проявления этих элементов определяют природу противодействия расследованию преступлений в сфере компьютерной информации.

4. Понятие «субъект, оказывающий противодействие расследованию» охватывает не только обвиняемого / подозреваемого в совершении преступления, но и иных лиц, которые в силу различных причин могут быть заинтересованы в определенном исходе уголовного дела (родственники обвиняемого / подозреваемого; потерпевшие, считающие, что проводимым расследованием может быть нанесён вред их деловой репутации; отдельные активные пользователи глобальных компьютерных сетей, которые считают своим долгом помочь виновному в уходе от уголовной ответственности).

5. В силу того, что преступления в сфере компьютерной информации чаще всего совершаются с использованием глобальных компьютерных сетей, основным средством, которое используется для противодействия расследованию данных преступлений, также являются эти сети. С этой целью используются специальные программы, которые помогают посредством этих сетей либо сокрыть, либо инсценировать совершённое преступление. Также глобальные компьютерные сети могут выступать в качестве средства противодействия расследованию конкретного преступления с целью формирования благоприятного для обвиняемого (подозреваемого) общественного мнения, посредством которого можно было бы воздействовать на следователя и иных лиц, оказывающих ему содействие.

6. Для способов сокрытия преступлений в сфере компьютерной информации характерно следующее:

- в качестве основных средств сокрытия используются такие компьютерные программы, которые помимо возможности совершить соответствующее преступление, позволяют не оставлять следов его совершения, а те, которые остаются, - уничтожают, так, чтобы никто не мог догадаться о том, что было совершено какое-то противоправное посягательство;

- подбираются программы, которые делают невозможным установление личности лица, совершившего конкретное преступление;

- для сокрытия преступления подбираются компьютерные программы, которые не могут выявить системы безопасности;

- для обеспечения тайности проникновения в информационную систему могут использоваться отвлекающие манёвры (например, хакерские атаки, которые призваны только сконцентрировать на себе внимание);

- использование технических возможностей в сокрытии преступления согласовывается и обеспечивается также и другими методами и средствами (например, создаётся ситуация, когда потерпевшему невыгодно привлекать к себе внимание из-за совершённого преступления, так как это может нанести ущерб его репутации).

7. Место противодействия расследованию преступлений в сфере компьютерной информации - это не только определённая местность или помещение, в котором предприняты и совершены действия, направленные на противодействие расследованию конкретного преступления, но и место входа в компьютерную информационную систему, а также место в самой

этой информационной системе, в которой совершается противодействие расследованию.

8. Обстановка противодействия расследованию компьютерных преступлений – это совокупность технологических условий функционирования конкретной виртуальной реальности независимо от того, где эта реальность имеет место – в локальной информационной системе или в информационной сети.

9. Преодоление противодействия расследованию преступлений в сфере компьютерной информации на стадии возбуждения уголовного дела предполагает решение следующих задач:

1) обеспечение конфиденциальности при сборе информации о совершённом преступлении и о виновных в его совершении лицах;

2) сбор информации о лицах, которые имеют доступ к документам (в том числе электронным) и которые могут предпринять действия, по уничтожению уличающих конкретное виновное лицо доказательств;

3) определение следователем задач поиска информации, необходимой для решения вопроса о возбуждении уголовного дела;

4) установление источников, из которых в ходе последующего предварительного расследования могут быть получены доказательства о конкретном преступлении в сфере компьютерной информации и лице, виновном в его совершении;

5) прогнозирование возможного противодействия проведению действий по сбору материала для решения вопроса о возбуждении уголовного дела;

6) планирование и проведение упреждающих противодействие действий;

7) планирование и проведение действий по преодолению уже оказываемого расследованию противодействия.

10. Для успеха преодоления противодействия расследованию преступлений в сфере компьютерной информации необходимо выполнение требований по обеспечению тайны проводимых действий:

1) ограничить, а в отдельных случаях сделать невозможным вход и выход с компьютеров, на которых имеется информация, на которую было направлено преступное посягательство, в глобальные сети. Это необходимо для того, чтобы никто не мог, пользуясь глобальными сетями, узнать действия, производимые на конкретном компьютере;

2) если конкретным пострадавшим от преступления юридическим лицом в глобальной сети велась какая-то деятельность (блог, сайт и т. п.), необходимо продолжать её с тем, чтобы не привлекать к действиям, направленным на расследование преступления, излишнего внимания;

3) определить последовательность действий, направленных на расследование преступлений, так, чтобы действия к лицам, которые, по мнению следователя, могут исказить или рассекретить полученную информацию, были совершены в последнюю очередь, лишь после того, когда будет в основном сформирована доказательственная база. Так, предъявлять

обвинение, а также выполнять действия, в результате которых лицо может быть признано подозреваемым (ч. 1 ст. 46 УПК РФ), следует по времени ближе к окончанию проводимого расследования;

4) обыск или выемку проводить в то время, когда можно избежать присутствия большого количества очевидцев;

5) к проведению следственных действий в качестве понятых привлекать желательно лиц, не связанных с деятельностью конкретного юридического лица, или, если это физическое лицо, они не должны быть знакомы последнему;

6) необходимо осуществлять постоянный контроль за всеми исходящими через посредство глобальной компьютерной сети сообщениями из конкретного подразделения, группы, занятой расследованием конкретного преступления в сфере компьютерной информации. С этой целью вполне оправдано определение круга лиц, которому доступна информация о проводимом расследовании, и осуществление контроля за выходом этих лиц в глобальные компьютерные сети;

7) выявить дефекты в системе защиты информации в компьютере (компьютерах), принадлежащих потерпевшему, с тем, чтобы предотвратить возможность нового несанкционированного проникновения в систему, находящуюся в нем информацию, с целью уничтожения следов уже совершённого преступления или инсценировки;

8) выявить скрытые угрозы для системы информации, хранящейся на компьютере, на котором была изменена или уничтожена информация.

11. Правоохранительные органы должны предупреждать возможность противодействия расследованию, для чего необходима хорошо разработанная, эффективная стратегия и четко сформулированные задачи расследования. К названным задачам относятся следующие:

1) оперативно-розыскное обеспечение расследования преступлений;

2) обеспечение следственной тайны;

3) обеспечение взаимодействия между следователем и лицами, на которых возложена обязанность проведения оперативно-розыскных мероприятий с целью получения информации о готовящемся либо проводимом противодействии расследованию, и организация и проведение действий по упреждению или нейтрализации противодействия расследованию;

4) определение процессуальных и иных действий, которые могут иметь стратегическое значение в преодолении противодействия со стороны лиц, в нём заинтересованных;

5) определение порядка совершения как следственных, так и оперативно-розыскных мероприятий, который мог бы лишить обвиняемого (подозреваемого) и лиц, оказывающих ему содействие, возможности реализовать намерения по оказанию противодействия расследованию;

6) определение сочетания оперативно-розыскных мероприятий со следственными действиями, которое может предотвратить возможность оказания противодействия;

7) обеспечение общего руководства в преодолении противодействия расследованию следователем;

8) для планирования стратегии преодоления противодействия расследованию привлечение специалиста в сфере компьютерной информации;

9) для оказания эффективного преодоления противодействия расследованию необходимо в системе планируемых к выполнению действий предусмотреть мероприятия технического характера. Например, установление специальных программ защиты от несанкционированного проникновения в конкретную информационную систему; установка всевозможных фильтров, которые препятствуют проникновению в защищаемую информационную систему всевозможных вредоносных программ;

10) использование специальных технических средств для своевременного обнаружения противодействия расследованию и для его преодоления;

11) сочетание оперативно-розыскных мероприятий и процессуальных действий со специальными техническими средствами и возможностями, обеспечивающее эффективное преодоление оказываемого расследованию противодействия.

12. При расследовании преступлений в сфере компьютерной информации, наряду с допросом, ключевым следственным действием является выемка соответствующего носителя информации.

Специфика тактической операции «выемка носителей компьютерной информации, в отношении которой были совершены преступные действия», определяется особенностями:

1) предмета выемки;

2) круга участников;

3) характера совершаемых по изъятию действий.

Теоретическая значимость результатов исследования заключается в том, что сформулированные в диссертации теоретические положения и выводы вносят определенный вклад в развитие теории криминалистики в части изучения преодоления противодействия расследованию преступлений в целом и преступлений в сфере компьютерной информации, в частности. Кроме того, теоретические выводы и предложения, сформулированные в диссертационном исследовании, могут стать базой для дальнейших научных исследований проблем, связанных с преодолением противодействия расследованию преступлений в сфере компьютерной информации.

Практическая значимость исследования состоит в его прикладном характере. Сформулированные в диссертационном исследовании выводы и рекомендации ориентированы на их дальнейшее использование в деятельности правоохранительных органов по преодолению противодействия расследованию преступлений в сфере компьютерной информации. Они способны существенно повысить эффективность применения существующих методик расследования преступлений в сфере

компьютерной информации, а также могут быть полезны при преподавании курса криминалистики и соответствующих дисциплин специализации в высших юридических учебных заведениях, при разработке программ и учебных пособий, на занятиях по повышению квалификации работников правоохранительных органов.

Апробация и внедрение в практику результатов диссертационного исследования. Основные положения исследования изложены диссертантом в 16 научных статьях, 7 из которых опубликованы в рецензируемых журналах и изданиях, рекомендованных ВАК при Министерстве образования и науки РФ.

Результаты проведенной диссертационной работы обсуждались на заседаниях кафедры уголовного права, криминалистики и криминологии ФГБОУ ВПО «Мордовский государственный университет им. Н.П. Огарёва».

Теоретические положения и выводы диссертационного исследования были положены в основу выступлений на XXXIII Огаревских чтениях (Саранск, 2005), всероссийской научно-практической конференции «Актуальные проблемы совершенствования уголовно-правовых, криминалистических и криминологических мер борьбы с преступностью» (Саранск, 5-6 декабря 2005 года), I заочной всероссийской научно-практической конференции «Теория и практика правоприменительной деятельности: материалы» (Саранск, 2010), международной научно-практической конференции в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине» «Современные тенденции развития криминалистики и судебной экспертизы в России и Украине» (Белгород, 25-26 марта 2011), 7-ой международной научно-практической конференции «Ключови въпроси в съвременната наука» (София, 2011), международной научно-практической конференции, посвященной 35-летию со дня образования кафедры криминалистики Академии МВД Республики Беларусь (Минск, 3 июня 2011 г.); международной научно-практической конференции «Право и его реализация в XXI веке» (Саратов, 2011) .

Материалы диссертационного исследования внедрены в деятельность МВД Республики Мордовия. Апробация результатов исследования подтверждается соответствующими актами внедрения диссертационных положений в практику правоохранительных органов.

Структура и объём диссертации соответствуют требованиям ВАК при Министерстве образования и науки Российской Федерации и определены логикой достижения поставленной цели и задач проведённого исследования.

Диссертация состоит из введения, трёх глав, включающих десять параграфов, заключения, списка используемой литературы и приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, определяются его объект, предмет, цели, задачи, методологическая основа и эмпирическая база, сформулированы основные положения, выносимые на

защиту, аргументирована научная новизна, отражены теоретическая и практическая значимость, приведены сведения об апробации результатов проведённого диссертационного исследования.

Первая глава «Препятствия, затрудняющие расследование преступлений в сфере компьютерной информации» состоит из трех параграфов.

В первом параграфе «Понятие и виды препятствий в расследовании преступлений» обосновывается положение о том, что к факторам, затрудняющим расследование преступлений в сфере компьютерной информации, относится не только противодействие, но и целый ряд иных препятствий. При этом сведения об этих препятствиях должны являться информационной основой расследования преступлений в сфере компьютерной информации. Разрешение проблем, связанных с преодолением этих препятствий, осложняется целым рядом технических трудностей, обусловленных особенностями компьютеров и используемого в них программного обеспечения. Все препятствия, осложняющие расследование, можно подразделить на объективные и субъективные факторы. К объективным – следует отнести все те факторы, которые возникают и действуют независимо от воли конкретных лиц, кем бы они не были следователем или преступником. Возникают они в силу определённого стечения обстоятельств, которое является результатом действия объективно существующих сил или законов. К таким препятствиям следует отнести неблагоприятные природные условия, которые способствовали уничтожению следов преступления, или, к примеру, непредвиденная поломка механизма, который должен был бы использоваться при совершении преступления. К субъективным – следует отнести противодействие, которое оказывается со стороны лиц, совершивших преступление, и лиц, которые в силу различных причин не хотят, чтобы это преступление было раскрыто, а также ошибки следователя, ведущего расследование, и должностных лиц, содействующих этому расследованию. Практика расследования преступлений в сфере компьютерной информации позволяет сделать вывод о существовании ещё одной – третьей классификационной группы, которую можно назвать, как группа условно объективных факторов. К данной группе факторов следует относить особенности носителей компьютерной информации, которые могут стать причиной уничтожения этой информации, что, безусловно, препятствует расследованию преступлений в сфере компьютерной информации.

Также отмечается, что одним из основных мотивов совершения преступлений в сфере компьютерной информации является желание скрыть какое-либо иное преступление. С этих позиций становится понятным то, что совершение названного вида преступлений может быть, при определённых условиях, одним из элементов в системе преступных деяний, направленных на достижение определённой преступной цели. Это позволяет утверждать, что и сами преступления в сфере компьютерной информации могут

рассматриваться как один из способов преступного противодействия проводимому расследованию.

Во втором параграфе «Природа и механизм противодействия расследованию преступлений в сфере компьютерной информации» обосновывается то, что противодействие расследованию может быть не только противозаконным, но и законным. Так, в законе нет запрета обвиняемому использовать ходатайства для того, чтобы осложнить расследование преступления, сделать невозможным установление обстоятельств совершения конкретного преступления. Распространенными являются виды законного противодействия которые основаны на отсутствии необходимых знаний в области информационных технологий у сотрудников правоохранительных органов.

В связи с этим, наиболее часто с целью противодействия используются ходатайства о проведении тех или иных следственных действий, которые, якобы, могут стать источником получения ценной для установления обстоятельств дела информации. При этом, в данных ходатайствах обвиняемый и его защитник стремятся навязать следствию свою версию произошедшего, представив всё в виде «безобидных», неопасных для общества действий обвиняемого. Целью таких ходатайств является стремление «перегрузить» следователя информацией, чтобы он не смог в большом её объёме правильно сориентироваться, а, следовательно, самостоятельно определиться в том, какие сведения имеют отношение к делу, а какие - нет. В этом случае у обвиняемого и его защитника появляется возможность навязывать следователю своё видение ситуации и расследуемого события.

Другим наиболее распространенным видом законного противодействия расследования преступлений в сфере компьютерной информации являются показания самого обвиняемого, в которых он предлагает свою версию произошедшего. Чаще всего, при допросе обвиняемый вначале стремится определить степень осведомлённости следователя в сфере компьютерной информации, в целом, и в части совершённого преступления. Затем, на основе этой информации, он, чаще всего в ненавязчивой форме, стремится представить себя, либо как неискушённого в сфере компьютерной технике пользователя, либо, как лицо, которое неспособно иметь преступные цели, ввиду отсутствия у него «житейской хватки». Навязав такое представление о себе, обвиняемый как бы исподволь начинает преподносить следователю своё видение произошедшего, которое, как он пытается внушить, нельзя рассматривать как преступление.

Помимо названных видов противодействия расследованию преступлений в сфере компьютерной информации не менее распространенным является стремление обвиняемого и его защитника запутать следствие в терминологии, описывающей специфику информационных технологий, а также в процессах, которые используются в компьютерной технике. С этой целью - заявляются ходатайства о проведении всевозможных экспертиз, привлечению специалистов. С их помощью

делается попытка представить случившееся не как преступление, а как действие, допустимое, не противоречащее закону. Это достигается благодаря приёму, который именуется «подменой понятия». Он рассчитан на недостаточную осведомлённость следователя в сфере компьютерной информации.

Законное противодействие расследованию преступлений в сфере компьютерной информации не исчерпывается перечисленными видами.

Все виды законного противодействия классифицируются на: основанных на эмоциональных механизмах воздействия и - на рациональных (логических) механизмах. Первая группа видов противодействия основана на том, что с помощью перечисленных в законе средств защиты прав и законных интересов, можно воздействовать на эмоции лиц, участвующих в расследовании конкретного преступления. Вторая группа - основана на выстраивании в соответствии с определённой, логикой, имеющихся в уголовном деле фактов.

Психологическим механизмом, лежащим в основе противодействия, является конфликт между предполагаемым преступником и лицами, проводящими расследование. Данный вид конфликтов по принятой в юридической конфликтологии классификации следует относить к уголовно-процессуальным. Природа противодействия, раскрываемая в механизме конфликта, позволяет вскрыть его сущность и на этой основе определить методы, использование которых способно его нейтрализовать, обеспечив тем самым эффективность проводимого расследования.

В третьем параграфе «Основные формы противодействия расследованию преступлений в сфере компьютерной информации» обращается внимание на то, что следователи при расследовании преступлений в сфере компьютерной информации сталкиваются с вполне определённым набором форм противодействия их деятельности. Так, преступники, совершившие названный вид преступлений, обычно отдают предпочтение таким формам, как сокрытие и инсценировка. Наряду с этими формами противодействия преступниками используются и иные формы, среди которых, в частности, подкуп должностных лиц от которых зависит ход проводимого расследования. В последнее время достаточно широкое распространение получило воздействие на органы расследования, посредством формирования выгодного преступникам общественного мнения. При этом названные формы противодействия имеют особенности проявления, находящиеся в зависимости от особенностей преступлений в сфере компьютерной информации и от особенностей расследования этих преступлений. Так, сокрытию преступлений в сфере компьютерной информации во многом способствует то, что многие действия в этой сфере достаточно легко обезличиваются. Преступник уже в силу этого имеет возможность оставаться не выявленным. Одной из особенностей совершения преступлений в сфере компьютерной информации в последнее время стало использование в качестве средства совершения преступления существующих компьютерных сетей. Действия по сокрытию преступлений в сфере

компьютерной информации обычно выполняются одновременно с совершением самого преступления. Они предусматриваются преступниками уже на стадии подготовки конкретных преступлений названного вида и выполняются на всех стадиях его совершения. Причём одни и те же действия могут выполняться для достижения и общей преступной цели, которая определена в уголовном законодательстве для преступлений в сфере компьютерной информации, и для того, чтобы скрыть любые свидетельства о его совершении.

Среди инсценировок при совершении преступлений в сфере компьютерной информации наиболее распространены следующие:

- создание видимости того, что информация была повреждена в результате неумелого обращения с ней лиц, имеющих право доступа к ней;
- заражение вирусом лицами, имеющими доступ к компьютерной информации по неосторожности;
- вывод носителя информации из рабочего состояния, якобы, в результате действия причин, не зависящих от пользователя или иного лица (скачки электрического напряжения в сети и т.п.);
- имитация другого правонарушения в компьютерной сети с целью отвлечения внимания от действий, которыми преступник стремится добиться ожидаемого им криминального результата.

Во **второй главе «Структура противодействия расследованию преступлений в сфере компьютерной информации»** рассматриваются элементы структуры противодействия, которые являются, по существу, информационной основой для деятельности следователя по преодолению такого противодействия.

В первом параграфе «Общая характеристика структуры противодействия расследованию преступлений в сфере компьютерной информации» обращено внимание на факторы, определяющие эффективность оказываемого расследованию противодействия. К таким факторам следует отнести:

- субъекта, оказывающего противодействие расследованию;
- цель и мотив оказания противодействия;
- объект, на который направлено противодействия расследованию;
- средства и способ противодействия оказываемого расследованию;
- время, место, обстановка, в которых осуществляется противодействие расследованию;
- ошибки, допущенные следователем или лицами, содействующими ему в расследовании;
- деятельность третьих лиц или случайных факторов, которые могут быть использованы в ходе оказываемого противодействия.

Названный перечень факторов нельзя рассматривать, как исчерпывающий. Однако, именно он в наибольшей мере характеризует противодействие расследованию преступлений в сфере компьютерной информации. Названные факторы определяют структуру, оказываемого расследованию противодействия.

В зависимости от особенностей совершённого преступления противодействие его расследованию имеет свои индивидуальные особенности. Это определяет индивидуальность конкретного противодействия расследованию. При этом индивидуальность проявляется, в частности, в особенностях структуры противодействия расследованию отдельных видов преступлений. В этом случае она проявляется не в отсутствии, или, напротив, в наличии того или иного её элемента, а в его значимости для осуществляемого противодействия расследованию. Значимость, в свою очередь, зависит от силы и интенсивности действия фактора, который входит в названную структуру в качестве её элемента. Также определяющей индивидуальность структуры противодействия расследованию всякого преступления являются особенности каждого из элементов её составляющих. Индивидуальность структуры противодействия зависит от индивидуальности её элементов. Другой особенностью индивидуализирующей структуру противодействия расследования различных преступлений являются особенности связей между её элементами. Так, для личности субъекта противодействия расследованию преступлений в сфере компьютерной информации характерно культивирование интеллектуальных свойств личности. Это определяет и характер связи между субъектом противодействия и способом совершения противодействия.

Во втором параграфе «Субъекты противодействия расследованию преступлений в сфере компьютерной информации» определяется круг лиц, охватываемый понятием «субъект противодействия расследованию преступлений в сфере компьютерной информации» и рассматриваются особенности этого субъекта. Одной из особенностей субъекта противодействия является то, что им может быть не только обвиняемый (подозреваемый), но и иные лица. В частности, это может быть родственник подозреваемого (обвиняемого), его друг или приятель, либо иное лицо, которое, в отдельных случаях, даже не из корысти считает необходимым оказать ему помощь в уклонении от уголовной ответственности. Более того, в отдельных случаях оказывать противодействие расследованию может даже потерпевший от этого преступления. При этом личность преступника, оказывающего противодействие, обладает определёнными качествами, которые позволяют выделять её в эту особую классификационную группу. Для лиц, оказывающих противодействие расследованию преступлений в сфере компьютерной информации характерно наличие следующих качеств:

- высокая стрессоустойчивость, проявляющаяся в том, что, несмотря на повышенную реальную опасность разоблачения и наказания за совершённое преступление, названные лица проявляют самообладание, необходимое для принятия верных решений;

- способность сконцентрироваться в критических ситуациях для поиска наиболее эффективных способов выхода из них;

- высокая критичность в оценке складывающейся ситуации, позволяющая выбрать адекватные ситуации действия;

- эмоциональная устойчивость, позволяющая избегать решений, принимаемых на основе испытываемых сильных эмоций. В 100% случаев, не имеется сведений о стоянии преступника в наркологическом или психоневрологическом диспансере;

- уверенность в своём интеллекте и в своих силах, позволяющая не опасаться быть разоблачённым в оказываемом противодействии;

- наличие высокого интеллекта, позволяющего состязаться с интеллектом следователя или иного лица, которое оказывает содействие в расследовании соответствующего преступления в сфере компьютерной информации.

В третьем параграфе «Способ противодействия расследованию преступлений в сфере компьютерной информации» определяются характерные черты способа противодействия расследованию преступлений в сфере компьютерной информации, его особенности. Действия по совершению преступления и действия по его сокрытию часто объединены единым умыслом, а потому одни и те же действия могут являться, как способом совершения конкретного преступления, так и способом сокрытия этого же преступления. Способ противодействия расследованию, как правило, бывает обусловлен способом совершения преступления. Справедливо и обратное – способ совершения преступления часто бывает обусловлен последующим способом противодействия расследованию.

Для всех способов сокрытия преступлений в сфере компьютерной информации характерно следующее:

- в качестве основных средств сокрытия используются компьютерные программы, которые помимо возможности совершить соответствующее преступление, позволяют не оставлять следов его совершения, а те которые остаются - уничтожают, так чтобы никто не мог даже догадаться о том, что что-то было совершено;

- в тех случаях, когда всё же не представляется возможным полного уничтожения названных следов, подбираются программы, которые делают невозможным установление личности лица, совершившего конкретное преступление;

- для сокрытия преступления подбираются компьютерные программы, использование которых, по мнению преступника, не могут выявить системы безопасности, которые должны пресекать возможность несанкционированного входа в охраняемую информационную систему;

- для обеспечения тайности проникновения в информационную систему могут использоваться отвлекающие манёвры (например, хакерские атаки, которые призваны только сконцентрировать на себе внимание);

- использование технических возможностей в сокрытии преступления, согласовываются и обеспечиваются также и другими методами и средствами (например, создаётся ситуация, когда потерпевшему невыгодно привлекать к себе внимание из-за совершённого преступления, так как это может нанести ущерб его репутации).

В четвёртом параграфе «Иные элементы структуры противодействия расследованию преступлений в сфере компьютерной информации» рассмотрены такие элементы структуры противодействия расследованию преступлений в сфере компьютерной информации, как место, время и обстановка совершения противодействия, ошибки, которые допускаются при расследовании, действия третьих лиц. При этом, названные элементы структуры были определены в соответствии с их значением для деятельности по преодолению противодействия расследованию. Так, с учётом того, что место совершения преступления предполагает его одновременное нахождение в предметном и виртуальном мире, место противодействия также будет находиться в виртуальном и реальном мире, в частности, в случаях сокрытия или инсценировки конкретного преступления в сфере компьютерной информации. Такая двойственность определения места сокрытия или инсценировки предполагает то, что для выявления данных действий необходимо в равной мере уделять внимание предметной и виртуальной действительности. Обстановка противодействия расследованию преступлений в сфере компьютерной информации охватывает технологические условия функционирования конкретной виртуальной реальности независимо от того, где эта реальность имеет место – в локальной информационной системе или в информационной сети.

Ошибки, допущенные следователем при расследовании преступлений в сфере компьютерной информации, существенным образом влияют на складывающуюся следственную ситуацию. Результатом их совершения является формирование неблагоприятных для правоохранительных органов следственных ситуаций, которыми незамедлительно стремятся воспользоваться лица, противодействующие проводимому расследованию. То есть, неблагоприятная следственная ситуация используется, как основа для планирования противодействия расследованию конкретного преступления. Поэтому вполне очевидно, что допущенная при расследовании следователем ошибка может сформировать момент перелома хода расследования в пользу лиц (лица) совершившего преступление.

Действия третьих лиц, в отдельных случаях, также препятствуют эффективному расследованию преступлений в сфере компьютерной информации. Всех третьих лиц, которые оказывают противодействие расследованию преступления можно условно разделить на следующие группы:

1) родственники, которые в силу близости своих отношений с преступником готовы совершать самые разнообразные действия с целью не допустить привлечения к уголовной ответственности виновного. При этом они могут быть убеждены в невиновности такого лица, а потому оказывать содействие в противодействии, считая, что тем самым способствую также и правосудию;

2) друзья, товарищи, коллеги по работе. Для этой категории, как правило, характерна абсолютизация принципов, на которых строятся дружеские отношение. Они считают, что друга необходимо поддерживать

всегда и всеми способами несмотря даже на то, что друг совершает преступление;

3) лица, которые опасаются разглашения сведений, которые могут поставить под удар их доброе имя и репутацию. Перечень таких лиц чрезвычайно широк. К ним, в частности, могут относится и потерпевшие от конкретного преступления, когда сами потерпевшие считают, что если определённая информация станет достоянием следственных органов и, следовательно, неопределённого количества иных лиц, их имидж может пострадать.

В **третьей главе «Тактические и стратегические основы преодоления противодействия расследованию преступлений в сфере компьютерной информации»** рассматриваются наиболее проблемные вопросы тактики и стратегии преодоления противодействия расследованию преступлений в сфере компьютерной информации, предлагаются рекомендации, которые могут обеспечить эффективность действий по преодолению названного противодействия.

В **первом параграфе «Преодоление и нейтрализация противодействия расследованию преступлений в сфере компьютерной информации. Преодоление противодействия на стадии возбуждения уголовного дела и предварительного расследования»** указывается на то, что действия по преодолению противодействия имеют отличия в зависимости от того, на какой стадии уголовного процесса они совершаются. Поэтому следует выделять с учётом этого основания: 1) преодоление противодействия на стадии возбуждения уголовного дела и 2) преодоление противодействия на стадии предварительного расследования. При этом, преодоление противодействия на стадии возбуждения уголовного дела связано с тем, что преступник и лица, желающие оказать ему содействие, стремятся к тому, чтобы преступление оставалось скрытым от правоохранительных органов. Выявление преступления в значительной мере связано не только с деятельностью следователя, но и соответствующих оперативных подразделений правоохранительных органов. Поэтому противодействие направлено, прежде всего, против деятельности сотрудников этих подразделений. Спецификой возбуждения уголовного дела по преступлениям в сфере компьютерной информации является то, что уже на этой стадии со стороны преступников и лиц, им сочувствующих, оказывается достаточно серьёзное противодействие. Поэтому, проводимые оперативно-розыскные мероприятия часто преследуют решение не только задач сбора необходимой для решения вопроса о возбуждении уголовного дела информации, но и задач, связанных с необходимостью преодоления противодействия такому сбору информации. Преодоление противодействия на стадии возбуждения уголовного дела о преступлениях в сфере компьютерной информации предполагает решение следующих задач:

1) обеспечение конфиденциальности при сборе информации о совершённом преступлении и о виновных в его совершении лицах;

2) сбор информации о лицах, которые имеют доступ к документам (в том числе электронным), и которые могут предпринять действия, по уничтожению уличающих конкретное виновное лицо доказательств;

3) определение следователем задач поиска информации, необходимой для решения вопроса о возбуждении уголовного дела;

4) установление источников, из которых в ходе последующего предварительного расследования могут быть получены доказательства о конкретном преступлении в сфере компьютерной информации и лице, виновном в его совершении;

5) прогнозирование возможного противодействия проведению действий по сбору материала для решения вопроса о возбуждении уголовного дела. Для этого необходимо использовать рефлексивные рассуждения, которые позволяют предвидеть поведение преступника;

6) планирование и проведение упреждающих противодействие действий;

7) планирование и проведение действий по преодолению уже оказываемого расследованию противодействия.

На стадии предварительного расследования у следователя появляется гораздо больше возможностей по преодолению противодействия. Однако, как правило, и обвиняемый на этой стадии активизирует свою деятельность по противодействию расследованию. Необходимо, чтобы активно проводилась оперативная работа по установлению намерений заинтересованных в противодействии лиц, планируемых ими действий, которыми они стремятся осложнить установление истины по уголовному делу. В этом случае следователь может своевременно предпринять действия на опережение, которыми предвосхитит планируемое противодействие, сделает его неэффективным.

Во втором параграфе «Стратегия и тактика преодоления противодействия расследованию преступлений в сфере компьютерной информации» рассмотрены основные направления по решению проблем стратегии и тактики преодоления противодействия расследованию преступлений в сфере компьютерной информации. Следователь должен исходить из того, что помимо противодействия охватывающего собой только отдельное следственное действие или оперативно-розыскное мероприятие преступник и оказывающие ему помощь лица предусматривают длительную систему действий по противодействию расследованию преступлений. Разработанный на первоначальном этапе расследования план позволяет оказывать преодоление противодействию на долгосрочной основе, и обеспечить успех проводимого расследования. Стратегическими задачами преодоления противодействия расследованию является наиболее оптимальный подбор и планирование действий, опирающийся на выяснение складывающейся следственной ситуации и прогнозы по её изменению, способных предотвратить наступление неблагоприятных для установления истины по делу последствий. Для преодоления противодействия

расследованию преступлений в сфере компьютерной информации необходимо решение следующих задач:

1) для планирования стратегии преодоления противодействия расследованию необходимо привлекать специалиста в сфере компьютерной информации;

2) для оказания эффективного преодоления противодействия расследованию необходимо в системе планируемых к выполнению действий предусмотреть мероприятия технического характера. Под такими мероприятиями понимается выполнение действий по установлению специальных программ защиты от несанкционированного проникновения в конкретную информационную систему; установка всевозможных фильтров, которые препятствуют проникновению в защищаемую информационную систему всевозможных вредоносных программ. Могут применяться программы, помогающие в определении следов несанкционированного доступа и их идентификации;

3) использование специальных технических средств для своевременного обнаружения противодействия расследованию и для его преодоления;

4) сочетание оперативно-розыскных мероприятий и процессуальных действий со специальными техническими средствами и возможностями, обеспечивающее эффективное преодоление оказываемого расследованию противодействия.

Отмечая необходимость определения стратегии по преодолению противодействия со стороны обвиняемого (подозреваемого) и лиц, оказывающим ему содействие, для решения задач расследования, нельзя не отметить важности и вопросов тактики преодоления такого противодействия. Среди значимых следственных действий и с точки зрения стратегии расследования является выемка.

В третьем параграфе «Тактические приёмы, тактические операции и тактические комбинации при преодолении противодействия расследованию преступлений в сфере компьютерной информации» рассматриваются проблемы теории и практики по преодолению противодействия расследованию преступлений в сфере компьютерной информации с помощью тактических приёмов, тактических операций и тактических комбинаций. Большое значение для расследования преступлений в сфере компьютерной информации имеют следующие тактические операции:

1) выемка носителей компьютерной информации, в отношении которой были совершены преступные действия;

2) предъявление обвинения виновному лицу в совершении преступления в сфере компьютерной информации и его допрос;

3) обыск с целью изъятия носителей компьютерной информации, в отношении которой были совершены преступные действия.

Спецификой тактической операции «выемка носителей компьютерной информации, в отношении которой были совершены преступные действия» является:

1) специфика предмета выемки. Это может быть любой носитель компьютерной информации, на котором находится или могла находиться (по имеющимся данным) искомая компьютерная информация;

2) круг участников данной тактической операции. Он отличается тем, что помимо следователя и сотрудников правоохранительных органов, на которых возложена обязанность проведения оперативно-розыскных мероприятий, привлекаются специалисты в области компьютерной техники и информатики;

3) характер, совершаемых в ходе выемки действий. Так, данная тактическая операция должна в себе сочетать одноимённое следственное действие, оперативно-розыскные мероприятия, действия технического характера.

Также рассмотрены особенности проведения тактической операции «предъявление обвинения виновному лицу в совершении преступления в сфере компьютерной информации и его допрос». На основе этого предлагаются рекомендации по преодолению противодействия расследованию названного вида преступлений.

В **заключении** сформулированы основные выводы диссертационного исследования, наиболее значимые из которых изложены в тексте настоящего автореферата при обобщении материала соответствующих глав и параграфов.

Основные положения диссертации отражены в следующих публикациях автора:

- *статьи в рецензируемых научных журналах и изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки РФ для опубликования основных научных результатов диссертаций:*

1) *Косынкин, А.А., Подольный, Н.А.* Личность лица, совершающего преступления в сфере компьютерной информации / А.А. Косынкин, Н.А. Подольный // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Право. - Выпуск 2(10). Уголовное судопроизводство в теории, законодательстве и конкретных жизненных ситуациях. - Н. Новгород : изд-во ННГУ, 2006. - С. 291-294 (в соавторстве, авторство не разделено, 0,2 п.л.);

2) *Косынкин, А.А.* Противодействие расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Следователь. - М. : Честь и закон, 2007. - №3. - С. 22-26 (0,45 п.л.);

3) *Косынкин, А.А.* Особенности личности лица, совершающего преступления в сфере компьютерной информации / А.А. Косынкин // Следователь. - М. : Честь и закон, 2007. - №10. - С. 46-48 (0,2 п.л.);

4) *Косынкин, А.А.* Очная ставка как способ преодоления противодействия следователем при расследовании преступлений в сфере

компьютерной информации / А.А. Косынкин // Следователь. - М. : Честь и закон, 2008. - №2. - С. 59-62 (0,27 п.л.);

5) *Косынкин, А.А.* Соотношение конфликта и противодействия при расследовании преступлений в сфере компьютерной информации / А.А. Косынкин // Российский следователь. - М. : изд. группа «Юрист», 2011. - №10. - С. 28-30 (0,24 п.л.);

6) *Косынкин, А.А.* Инсценировка как форма противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Вестник Челябинского государственного университета. - Челябинск : изд-во «ЧелГУ», 2011. - №29 (244). Право. Вып. 29. - С. 78-80 (0,33 п.л.);

7) *Косынкин, А.А.* Результат противодействия как элемент структуры противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Проблемы права. – Челябинск : НП «Южноуральский юридический вестник», 2011. - № 4. - С. 155-159 (0,32 п.л.);

- *статьи в иных научных журналах и изданиях:*

8) *Косынкин, А.А.* Общая криминалистическая характеристика преступлений в сфере компьютерной информации / А.А. Косынкин // XXXIII Огаревские чтения : материалы науч. конф. : В 2 ч. Ч.1. Гуманитарные науки / сост. О.И. Скотников; отв. за вып. В.Д. Черкасов. – Саранск : изд-во Мордовского ун-та, 2005. - С. 228-231 (0, 23 п.л.);

9) *Косынкин, А.А.* Механизм совершения кардинга / А.А. Косынкин // Гуманитарные науки: в поисках нового : Межвуз. сб. науч. тр. - Вып.IV. – Саранск : Ковылк. тип., 2005. - С. 57-60 (0, 21 п.л.);

10) *Косынкин, А.А.* Осмотр места происшествия при расследовании преступлений в сфере компьютерной информации / А.А. Косынкин // Актуальные проблемы совершенствования уголовно-правовых, криминалистических и криминологических мер борьбы с преступностью : материалы Всерос. науч.-практ. конф. 5-6 декабря 2005 года / Морд. гос. ун-т им. Н.П .Огарева / под ред. П.В. Малышкина. – Саранск : Тип. «Руз.печ», 2006.- С. 297-302 (0,37 п.л.);

11) *Косынкин, А.А.* Планирование расследования преступлений в сфере компьютерной информации / А.А. Косынкин // Социальные и гуманитарные исследования: традиции и реальности : межвуз. сб. науч. тр. - Вып. V. – Саранск : Ковылк. тип., 2007. - С. 51-55 (0, 27 п.л.);

12) *Косынкин, А.А.* Проблемы преодоления противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Социальные и гуманитарные исследования: традиции и реальности : межвуз. сб. науч. тр. - Вып.VI. - Саранск : Ковылк. тип., 2007. - С. 30-33 (0, 2 п.л.);

13) *Косынкин, А.А.* Некоторые аспекты организации взаимодействия следователя со сведущими лицами в области компьютерных технологий для

преодоления противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Теория и практика правоприменительной деятельности : материалы I заоч. Всерос. науч.-практ. конф. / редкол.: А.М. Ахметова (отв. ред.) [и др.]. - Саранск : изд-во Мордовского ун-та, 2010. - С.152-156 (0, 25 п.л.);

14) *Косынкин, А.А.* Проблемы преодоления противодействия при расследовании преступлений в сфере компьютерной информации // Современные тенденции развития криминалистики и судебной экспертизы в России и Украине : материалы Междунар. науч.-практ. конф. В рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», 25-26 марта 2011г.: в 2 т. / отв. ред. И.М. Комаров. - Т. I. - Белгород : изд-во БелГУ, 2011. - С. 273-277 (0, 24 п.л.);

15) *Косынкин, А.А.* Преступление в сфере компьютерной информации, как действие, направленное на противодействие расследованию преступлений / А.А. Косынкин // Материали за 7-а международна научна практична конференция, «Ключови въпроси в съвременната наука». - Т. 21. Икономики. София : «Бял ГРАД-БГ» ООД, 2011. - С. 77-81 (0, 21 п.л.);

16) *Косынкин, А.А.* Природа и виды законного противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Актуальные проблемы современной криминалистики и судебной экспертизы : материалы Междунар. науч.-практ. конф., посв. 35-летию со дня образования кафедры криминалистики Акад. МВД Респ. Беларусь (Минск, 3 июня 2011 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования "Акад. М-ва внутр. дел Респ. Беларусь" ; редкол. [Н.И. Порубов и др.]. – Минск : Акад. МВД, 2011. - С. 157-159 (0,44 п.л.).