УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
"АКАДЕМИЯ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ"

УДК 343.985.7

ЛЕПЁХИН АЛЕКСАНДР НИКОЛАЕВИЧ

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.00.09 – уголовный процесс, криминалистика и судебная экспертиза;
оперативно-розыскная деятельность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Минск, 2007

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации

Эволюция социальной активности граждан выступает одним из основных факторов возникновения сложного комплекса проблем, обусловленных прогрессом общества. Качественные преобразования общественной жизни, и в первую очередь, развитие научно-технического прогресса, создают объективные условия для роста количества преступлений против информационной безопасности, что является негативной тенденцией, присущей любому современному обществу. Развитие компьютерных технологий и повышение их роли в современной жизни человечества, возрастание уровня овладения компьютерной техникой обуславливают внедрение компьютерных систем практически во все сферы деятельности человека. Такие тенденции, как появление компьютерной техники с огромными производительными возможностями, широкая функциональность ее применения, предопределяют компьютеризацию управленческой и экономической сфер жизни общества и необходимость более тщательного подхода к обеспечению безопасного функционирования компьютерных систем.

Прерогативой деятельности правоохранительных органов при решении задач быстрого и полного расследования преступлений, защиты личности, ее прав и свобод, а также интересов общества и государства является реализация принципа неотвратимости наказания. В самом общем виде сложность проблемы расследования преступлений против информационной безопасности объясняется специфичностью и новизной рассматриваемых противоправных деяний, многообразием способов криминальных посягательств, сложностью сбора и закрепления доказательной базы, мощным противодействием со стороны правонарушителей, что создает для правоохранительных органов существенные преграды в защите прав граждан, интересов общества и государства от противоправных действий. Кроме того, как показывает проведенное исследование, рассматриваемой группе преступлений присуща высокая латентность, которая зависит от специфики предмета преступного посягательства, что обуславливает необходимость овладения сотрудниками правоохранительных органов специальными знаниями в этой сфере, а также нежелания потерпевшей стороны в ряде случаев обращаться в правоохранительные органы.

Результаты исследования эмпирической базы свидетельствуют, что правоохранительная система оказалась не готова к бурному росту информационных технологий, их внедрению в большинство сфер жизни современного общества и к появлению связанных с ними правонарушений. Об этом свидетельствуют результаты изучения мнения работников правоохранительных органов по вопросам расследования преступлений против информационной безопасности, проведенные в 2004 и 2006 годах. Так, на вопрос анкеты: “По вашему мнению, готовы ли Вы процессуально грамотно осуществить действия по обнаружению, фиксации и изъятию компьютерной информации?”, – 78,1 % (2004 г.) и 72,4 % (2006 г.) опрошенных сотрудников дали отрицательный ответ. Причинами та-

кого положения являются: отсутствие комплексной теоретической основы криминалистического обеспечения расследования преступлений в этой сфере и, как следствие этого, недостаточная подготовка сотрудников правоохранительных органов по вопросам информационной безопасности.

В этой связи актуальной представляется разработка проблем расследования преступлений против информационной безопасности, чему и посвящена тема диссертационной работы, актуальность которой определяется:

- ростом количества криминальных деяний, обусловленным уязвимостью информационной сферы для преступных посягательств;
- особым характером общественно опасных последствий преступлений этого вида и значительным размером причиняемого ущерба;
- целесообразностью использования новых подходов к структуре частной криминалистической методики расследования криминальных деяний против информационной безопасности;
- обоснованностью формирования системы правовых основ расследования и исследования особенностей применения правовых норм;
- необходимостью выявления сущности преступлений против информационной безопасности с целью установления внутренних связей между элементами криминалистической структуры этого вида криминальных деяний и их познанием;
- сложностью процесса расследования преступлений против информационной безопасности в силу недостаточности конкретных практически значимых рекомендаций по проведению следственных действий.

При выборе представленного направления исследования мы исходили, с одной стороны, из современного состояния научных разработок по данной проблеме и, с другой, из практического значения формирования теоретических основ расследования преступлений против информационной безопасности в отечественной криминалистике для совершенствования деятельности органов предварительного расследования.

Связь работы с крупными научными программами, темами

Исследование выполнено в рамках пятилетнего перспективного плана (2006-2010 гг.) научно-исследовательской работы Академии МВД по разделу 1, п. 1.1. (по заданию МВД Республики Беларусь); плана научно-исследовательской работы Академии МВД на 2006 г. по разделу 1, п. 1.1; разделу 2, п. 2.5, п. 2.5.2 согласно п. 2.5 перспективного плана научно-исследовательской работы Академии МВД Республики Беларусь по 2010 г. Тема исследования согласуется с п.1.11 перечня актуальных направлений диссертационных исследований в области права по специальности 12.00.09, утвержденного решением Межведомственным советом по проблемам диссертационных исследований в области права от 09.02.2006 г.

Цель и задачи исследования

Целью исследования является разработка новых подходов к структуре частной криминалистической методики и выработка на основе полученных теоре-

тических положений научно-практических рекомендаций по расследованию преступлений против информационной безопасности.

Для достижения поставленной цели необходимо было решить следующие задачи:

- проанализировать современные научные представления по методике расследования преступлений против информационной безопасности и сформировать новый подход к структуре частной криминалистической методики рассматриваемого вида криминальных деяний;

- изучить содержание правовых основ расследования преступлений в данной сфере и предложить научно обоснованные рекомендации по совершенствованию законодательства;

- сформировать криминалистическую структуру преступлений против информационной безопасности и определить ее содержательное наполнение;

- разработать новый подход к организации расследования в форме теоретико-прикладной модели расследования криминальных деяний против информационной безопасности в условиях типичной следственной ситуации и разработать практические рекомендации по её использованию;

- исследовать тактические особенности проведения отдельных следственных действий при расследовании преступлений в сфере информационной безопасности и сформировать предложения по их осуществлению.

Объект и предмет исследования

Объектом исследования являются правоотношения, которые возникают, развиваются и прекращаются в связи с деятельностью органов уголовного преследования по расследованию преступлений против информационной безопасности.

Предмет исследования составляют закономерности совершения преступлений против информационной безопасности, а также теоретические, правовые и прикладные аспекты их расследования.

Методология и методы проведенного исследования

В процессе исследования использован комплекс философских (диалектико-материалистический), общенаучных (анализа и синтеза, системно-структурный, моделирования, исторический, экспериментальной проверки, логический) и специальных методов познания (социологический, сравнительно-правовой, включенного наблюдения).

Теоретической и методологической основой исследования послужили труды таких отечественных и зарубежных исследователей как Т.В. Аверьянова, Н.Ф. Ахраменка, О.Я. Баев, И.И. Басецкий, Ю.М. Батурин, Р.С. Белкин, А.Н. Васильев, В.Б. Вехов, И.А. Возгрин, Ю.В. Гаврилин, А.В. Гортинский, Г.И. Грамович, Д.В. Гребельский, А.В. Дулов, А.М. Жодзишский, В.Ф. Ермолович, Г.А. Зорин, А.В. Касаткин, А.Н. Караханьян, В.Е. Козлов, Ю.Г. Корухов, В.В. Крылов, В.Д. Курушин, А.П. Леонов, В.А. Лукашев, Г.Н. Мухин, Н.С. Полевой, Н.И. Порубов, В.Ю. Рогозин, Е.Р. Россинская, А.С. Рубис, Н.А. Селива-

нов, Б.П. Смагоринский, Б.Х. Толеубекова, А.И. Усов, В.Б. Шабанов, В.П. Шиенок, Н.Г. Шурухнов, А.А. Эксархопуло, Н.П. Яблоков и др.

Информационной базой диссертационного исследования послужили статистические данные Информационно-аналитического управления МВД Республики Беларусь, уголовные дела, возбужденные по ст. 349-355 Уголовного кодекса Республики Беларусь, а также научные достижения в области криминалистики, уголовного процесса, теории оперативно-розыскной деятельности и других отраслей научного знания (уголовного права, криминологии, психологии, социологии).

Для обеспечения достоверности выводов в процессе исследования использованы следующие эмпирические материалы. За период 2002-2006 г. нами проведено:

- изучение 97 уголовных дел в Республике Беларусь, возбужденных по различным составам преступлений в сфере информационной безопасности с момента вступления в силу Уголовного кодекса Республики Беларусь 1999 г. и на отчетный период - 2005 г.[1];
- анкетирование 117 следователей органов предварительного расследования Министерства внутренних дел и прокуратуры, 48 работников службы дознания, 69 работников уголовного розыска и службы по борьбе с экономическими преступлениями, 42 работника Управления по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь (анкетирование проводилось в 2004 и 2006 годах);
- сравнительный анализ актов законодательства Беларуси и России по вопросам ответственности за преступления в рассматриваемой сфере.

Научная новизна и значимость полученных результатов

Научная новизна полученных в ходе исследования результатов определяется следующим:

- впервые в отечественной криминалистической науке проведено исследование деятельности органов уголовного преследования по расследованию преступлений против информационной безопасности и на основе полученных результатов предложены рекомендации по ее совершенствованию;
- впервые выявлены и систематизированы закономерности и характерные признаки преступлений против информационной безопасности, служащие основой для формирования новых подходов к построению частной криминалистической методики расследования преступлений;
- сформирован новый подход к построению структуры частной криминалистической методики, включающей в себя: информационную основу расследования преступлений, состоящую из уголовно-правовой квалификации противоправных деяний и криминалистической структуры преступлений данного вида, а также методическую основу расследования в форме теоретико-прикла-

[1] Разница между числовым значением изученных и зарегистрированных уголовных дел (827) обусловлена тем, что после возбуждения уголовных дел большинство из них было соединено по различным основаниям в одно производство.

ных моделей расследования в условиях типичной следственной ситуации и рекомендаций по осуществлению отдельных следственных действий, направленных на реализацию ее положений;

- впервые проанализировано содержание правовых основ расследования преступлений против информационной безопасности, установлена корреляционная связь между нормами права и эффективностью борьбы с преступлениями в рассматриваемой сфере и сформулированы предложения по их совершенствованию;

- сформулировано авторское определение криминалистической структуры преступления в сфере информационной безопасности и установлены закономерные связи между ее элементами: личностью преступника, способом противоправных действий, обстановкой реализации преступного замысла и объектами-носителями следов противоправной деятельности;

- предложен новый подход к организации расследования в форме теоретико-прикладной модели расследования преступлений в сфере информационной безопасности, содержание которой раскрывается через систему действий, имеющих функционально-деятельностное предназначение для анализа исходной информации; определения сложившейся следственной ситуации; выдвижения общих и частных версий; определения направлений расследования в данной следственной ситуации; возбуждения уголовного дела; формирования перечня обстоятельств, подлежащих доказыванию; определения очередности проведения следственных действий и иных мероприятий, направленных на установление обстоятельств совершенного преступления, а также сформированы практические рекомендации по ее реализации.

Научная значимость полученных результатов состоит в том, что на основе анализа и обобщения научных достижений и материалов правоохранительной практики усовершенствована частная криминалистическая методика расследования преступлений против информационной безопасности, слагающаяся из системы научно обоснованных рекомендаций по вопросам организации расследования и применения правовых и криминалистических средств и приемов при решении задач уголовного процесса. Кроме того, полученные результаты представляют собой теоретическую и методологическую основу для формирования частных методик расследования новых видов преступлений, в том числе с использованием информационных технологий.

Практическая (социальная и экономическая) значимость полученных результатов

Практическая значимость исследования определена Палатой представителей Национального Собрания Республики Беларусь, Главным управлением предварительного расследования МВД Республики Беларусь, Управлением Республики Беларусь по раскрытию преступлений в сфере высоких технологий МВД, Государственным экспертно-криминалистическим центром МВД Республики Беларусь, Институтом национальной безопасности Республики Беларусь, Академией МВД Республики Беларусь, выводы которых зафиксированы в

документах о внедрении. Использование приведенных в диссертации результатов в практической деятельности, законотворческой практике и учебном процессе позволит повысить эффективность расследования преступлений против информационной безопасности, уровень преподавания, создать качественно новые правовые предпосылки для регулирования правоотношений в исследуемой сфере.

Повышение эффективности работы расследованию указанных правонарушений направленно на защиту прав, законных интересов граждан и общества, что определяет социальную значимость полученных результатов.

Экономическую значимость от внедрения результатов исследования сложно выразить в денежном эквиваленте, однако полное, всестороннее, объективное и быстрое расследование преступлений приведет, наряду с другими положительными последствиями, к экономии расходов на процесс предварительного расследования, путем значительного сокращения временных затрат на выполнение должностных обязанностей, а также уменьшению размера ущерба, причиняемого рассматриваемыми криминальными деяниями.

Основные положения диссертации, выносимые на защиту

1. Структура частной криминалистической методики расследования преступлений против информационной безопасности состоит из двух неотъемлемых частей: информационной основы расследования преступлений, состоящей из уголовно-правовой квалификации противоправных деяний и криминалистической структуры преступлений данного вида, а также методической основы расследования в форме теоретико-прикладных моделей расследования в условиях типичной следственной ситуации и рекомендаций по осуществлению отдельных следственных действий, направленных на реализацию ее положений (данное положение имеет как научную, так и практическую потенцию; научная выражается в расширении исследовательских представлений и теоретической базы криминалистической науки, а практическая предполагает улучшение качества расследования преступлений и сокращение его сроков).

2. Для совершенствования правовых основ расследования преступлений против информационной безопасности необходимо внести в уголовное и административное законодательство следующие дополнения и изменения. Кодекс об административных правонарушения необходимо дополнить статьями: ст. 22.6.1 "Модификация компьютерной информации", ст. 22.6.2 "Неправомерное завладение компьютерной информацией". В Уголовном кодексе следует внести изменения в ст. 350 "Модификация компьютерной информации", а также дополнить нормами: ст. 349^1 "Несанкционированный доступ к компьютерной информации", ст. 350^1 "Модификация компьютерной информации", 352^1 "Неправомерное завладение компьютерной информацией" (указанные предложения позволят более дифференцированно подойти к оценке действий правонарушителей и сократить финансовые затраты правоохранительных органов на пресечение данных правонарушений путем сокращения объемов рабочего времени, затраченного сотрудниками на производство по материалам и уголовным делам).

3. Определение криминалистической структуры преступлений, которая представляет собой систему криминалистически значимых сведений, детерминированную результатами взаимодействия преступника с окружающей средой, полученную в ходе анализа и обобщения следственной и судебной практики и выступающую информационной основой для формирования рекомендаций по раскрытию и расследованию отдельных видов и групп преступлений (введение в научный оборот данного определения позволит расширить категориальный аппарат криминалистики и зафиксировать современные научно-исследовательские представления по рассматриваемой проблеме).

4. Криминалистическая структура преступлений против информационной безопасности формируется с учетом жесткой детерминированности составляющих её элементов и включает в себя обобщенную информацию, полученную в результате криминалистического анализа:

- объектов-носителей следов преступной деятельности;
- обстановки реализации преступного замысла с использованием информационных технологий;
- наиболее распространенных способов совершения противоправных деяний указанного вида;
- личности преступника в сфере информационной безопасности (данное положение направлено на формирование информационной основы расследования, которая выступает базой для выдвижения версий, определения особенностей организации расследования, а также правильного выбора следователем тактики проведения отдельных следственных действий).

5. Теоретико-прикладная модель расследования преступлений против информационной безопасности в условиях типичной следственной ситуации, содержание которой раскрывается через систему действий, имеющих функционально-деятельностное предназначение для анализа исходной информации; определения сложившейся следственной ситуации; выдвижения общих и частных версий; определения направлений расследования в данной следственной ситуации; возбуждения уголовного дела; формирования перечня обстоятельств, подлежащих доказыванию; определения очередности проведения следственных действий и иных мероприятий, направленных на установление обстоятельств совершенного преступления (реализация данного положения позволит существенно обогатить научные представления по вопросам организации и методического обеспечения расследования, а также сократить затраты рабочего времени и материальных ресурсов на выполнение служебных обязанностей сотрудниками правоохранительных органов путем эффективного использования сил и средств).

Личный вклад соискателя

Диссертационное исследование выполнено соискателем самостоятельно, ему принадлежат теоретические разработки, рекомендации и выводы, представленные в виде научных публикаций. Личный вклад диссертанта выразился в разработке новых подходов к организации расследования, построению част-

ной методики расследования преступлений против информационной безопасности, определении путей совершенствования правовых основ расследования, формировании криминалистической структуры преступлений указанного вида и создании на их основе теоретико-прикладной модели расследования преступлений против информационной безопасности и рекомендаций по её реализации. Автором подготовлены 7 научных статей, диссертация и автореферат.

Работы, опубликованные в соавторстве, содержат не менее 50% текста, лично написанного диссертантом.

Апробация результатов диссертации

Основные теоретические положения, выводы, практические рекомендации и предложения, сформулированные по результатам исследования, апробированы в практической деятельности и учебном процессе, обсуждены и одобрены при проведении:

- 7-й, 8-й международных конференций "Комплексная защита информации" (Минск, 2003, Валдай, 2004); ежегодных научно-практических конференций Академии МВД Республики Беларусь, посвященных Дню белорусской науки (2003-2004); международной научно-практической конференции: "Юридическая наука и образование в Республике Беларусь на современном этапе" (Гродно, 2003); международной научно-практической конференции: "Право Беларуси: истоки, традиции, современность" (Новополоцк, 2004); международной научно-практической конференции посвященной 80-летию со дня рождения профессора Л.Л. Каневского (Уфа, 2005); международной научной конференций молодых ученых: "Молодежь в науке – 2005" (Минск, 2005); международной научно-практической конференции: "Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы безопасности" (Калининград, 2006).

Опубликованность результатов

Основные положения диссертации опубликованы в 19 работах, из них: 7 статей в научных журналах (в том числе, 3 – за рубежом), 3 статьи в сборниках научных трудов, 8 – в материалах конференций и 1 – тезисах выступления на научных конференциях. Общий объем опубликованных материалов составляет 87 страниц, из них 63 страниц подготовлены лично автором.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, девяти разделов, заключения, списка использованных источников, приложений. Объем диссертации составляет 116 страниц, список использованных источников содержит 238 наименований на 17 страницах, 11 приложений на 46 страницах, 2 таблицы и 4 схемы. Общий объем работы составляет 185 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе "Теоретико-правовые основы криминалистического обеспечения расследования преступлений против информационной безопасности" показано развитие теоретико-правовых взглядов на проблему пре-

ступности в сфере информационной безопасности, а также определены правовые основы и условия эффективной борьбы с рассматриваемыми криминальными деяниями.

Анализ научных точек зрения и практики расследования уголовных дел в сфере информационной безопасности позволил установить, что современный этап развития мирового информационного сообщества, в том числе и нашей республики, характеризуется интенсивным развитием процессов информатизации, широким их внедрением во все сферы человеческой деятельности. Отличительной чертой данных явлений выступает постоянное увеличение числа субъектов, вовлеченных в указанные процессы.

При изучении научных публикаций по рассматриваемой проблеме выделяются следующие направления развития теоретико-правовых взглядов на проблему преступности в сфере информационной безопасности: разработка вопросов о понятии и сущности таких преступлений; совершенствование уголовно-правовых средств борьбы с ними; анализ криминалистических аспектов противодействия исследуемым криминальным деяниям.

В ходе проведенного исследования установлено, в настоящее время в Республике Беларусь отсутствуют комплексные работы, посвященные системному, научно обоснованному рассмотрению проблем расследования преступлений в рассматриваемой сфере. Подобные в некоторой степени исследования проводились в Российской Федерации и Украине, которые имеют уголовное законодательство отличающееся от белорусского. При таких условиях до практических работников доходят лишь отдельные рекомендации, которые не способны коренным образом повлиять на качество расследования уголовных дел данной категории.

Указанные обстоятельства обуславливают необходимость проведения комплексного изучения вопросов криминалистического обеспечения расследования преступлений против информационной безопасности, в рамках которого целесообразно осуществить исследование по следующим направлениям: формирование новых подходов к построению частной криминалистической методики расследования преступлений против информационной безопасности; изучение правовых основ расследования преступлений в рассматриваемой сфере и путей их совершенствования; определение наиболее значимых для процесса расследования элементов криминалистической структуры; на основе рассмотренных правовых основ и криминалистической структуры криминальных деяний построение теоретико-прикладных моделей расследования преступлений против информационной безопасности в условиях типичной следственной ситуации и разработка практических рекомендаций по проведению следственных действий, которые вызывают наибольшие сложности у практических сотрудников в их реализации.

Специфика расследования противоправных деяний против информационной безопасности обуславливает необходимость применения помимо Уголовного и Уголовно-процессуального кодексов еще и законов, ведомственных

нормативных правовых актов, которые раскрывают понятия, используемые в диспозициях уголовно-правовых норм, а также в ряде случаев и международных нормативных правовых актов. В силу этого, система правовых основ расследования преступлений в рассматриваемой сфере может быть представлена следующим образом: международные нормативные правовые акты, законы Республики Беларусь, нормативные правовые акты органов государственного управления.

Анализ практики расследования свидетельствует, что в целях единообразного применения норм уголовного законодательства, а именно главы 31 "Преступления против информационной безопасности" УК Республики Беларусь, а также разрешения спорных вопросов квалификации преступлений и устранения, тем самым, ошибок при расследовании противоправных деяний этого вида было бы обоснованным принятие Пленумом Верховного Суда Республики Беларусь постановления по результатам обобщения судебной практики применения законодательства по делам о преступлениях против информационной безопасности. В постановлении необходимо было бы отразить спорные вопросы квалификации, а также разъяснить основные понятия, используемые в уголовно-правовых нормах, касающиеся преступлений против информационной безопасности. Принятие такого постановления позволило бы единообразно применять законодательство в этой сфере и избегать ошибок в процессе расследования рассматриваемых преступлений.

Во второй главе "Криминалистическая структура преступлений против информационной безопасности" рассматривается криминалистическая структура как составляющая информационной основы расследования преступлений против информационной безопасности, проводится криминалистический анализ ее элементов: объекты-носители следов преступной деятельности; обстановка реализации преступного замысла с использованием информационных технологий; способы совершения противоправных деяний указанного вида; личность преступника в сфере информационной безопасности. Исследование показывает, что можно говорить о криминалистической структуре преступления в целом и криминалистической характеристике какого-либо ее отдельного элемента (например, личность преступника, способ совершения).

Отличительной особенностью понятия "криминалистическая структура" является наличие жесткой детеминированности между элементами системы, обусловленной особым характером внутренних связей. Также важно отметить, что системообразующим элементом при формировании криминалистической структуры преступления выступает исследование объектов-носителей следов преступной деятельности.

Информация, полученная в ходе анализа указанного элемента, позволяет определить те недостающие составляющие криминалистической структуры конкретного вида преступления, полное знание которых позволит установить истинный характер происшедшего события. Причем, установление этих элементов должно носить не абстрактный теоретизированный характер, а быть

направленным на решение конкретных практически значимых задач, возникающих в процессе раскрытия и расследования преступлений, и в первую очередь служить основой для выдвижения версий.

Следы криминальной деятельности в сфере информационной безопасности могут быть классифицированы следующим образом: материальные следы; идеальные следы; информационные (виртуальные) следы.

Правильная криминалистическая оценка объектов-носителей следов противоправной деятельности позволяет уже на первоначальном этапе расследования по исходным следственным данным создать информационную основу для выяснения механизма преступного события и осуществления расследования. Практика расследования свидетельствует, что ни одно уголовное дело, возбужденное по факту совершения криминального деяния в данной сфере, не может быть успешно завершено без тщательного изучения именно информационных (виртуальных) следов противоправного деяния. При этом основными взаимодействующими объектами при совершении данного вида преступлений являются, с одной стороны материальные объекты в виде средств компьютерной техники, с другой стороны информационные объекты в виде алгоритмов команд.

В ходе расследования противоправных деяний рассматриваемого вида значение обстановки выражается в возможности установления, при ее исследовании следов, указывающих на профессиональные качества правонарушителя, его квалификацию, а также в ряде случаев на личностные характеристики преступника; в выявлении закономерных связей между обстановкой совершения преступления, выбором определенного способа действий в зависимости от условий, в которых совершается криминальное деяние, профессиональными преступными качествами правонарушителя и результатом отражения взаимодействия данных элементов – следами противоправной деятельности. В целом исследование обстановки реализации преступного замысла позволяет определить, что явилось предметом преступного посягательства, на основе полученных сведений правильно квалифицировать криминальное деяние и применить соответствующую методику расследования.

К элементам обстановки реализации преступного замысла в сфере информационной безопасности, оказывающим влияние на механизм совершения преступлений, относятся: пространственно-временные, технические и социально-психологические факторы, а также наличие либо отсутствие системы защиты информации. При этом решающее значение для обеспечения информационной безопасности имеют именно социально-психологические факторы, в том числе уровень квалификации специалистов, обеспечивающих защиту информации, что обуславливает наличие корреляционной связи между уровнем профессиональной подготовки специалиста, существующей системой защиты информации и характером следов криминальной деятельности на месте происшествия. Характер такой связи выражается в том, что чем выше уровень профессиональной подготовки специалиста, обеспечивающего

защиту информации, тем более информативной будет "следовая картина" при исследовании обстановки совершения преступления.

Анализ научной литературы, а также практики расследования позволяет констатировать, что нецелесообразно выделять конкретные способы совершения преступлений против информационной безопасности ввиду многообразия приемов реализации преступного замысла. В то же время, в зависимости от направленности преступного посягательства возможно объединение противоправных действий в определенные группы способов, направленных на: несанкционированный доступ к информации в компьютерной системе, сети или на машинном носителе (компьютерной информации); модификацию информации в компьютерной системе, сети или на машинном носителе; уничтожение (блокирование) информации в компьютерной системе, сети или на машинном носителе или их самих; неправомерное завладение компьютерной информацией; незаконный оборот программных или аппаратных средств, предназначенных для получения несанкционированного доступа к компьютерной информации либо иных вредоносных программ; нарушение правил эксплуатации компьютерной системы или сети; на комплексное использование способов.

Проведенное исследование дает возможность выделить две основные группы преступников в сфере информационной безопасности: лица, основным мотивом поведения которых является самореализация, в том числе и в деструктивной форме, при довольно высоком уровне профессиональной подготовки; лица, у которых корыстная направленность при совершении преступлений является преобладающей (при этом степень овладения навыками в сфере компьютерных технологий может быть разной, от начинающего пользователя до профессионала).

Значение приведенной классификации для практического использования выражается, в первую очередь, в возможности определения по внешнеповеденческим признакам, к какой группе правонарушителей относится лицо, какие характерные особенности поведения им присущи. Одновременно с этим, установление подобных обстоятельств будет способствовать выработке наиболее оптимальной линии поведения сотрудников правоохранительных органов при проведении следственных действий.

При этом следует отметить, что мотивация преступников при длящемся характере преступной деятельности имеет эволюционный характер – от совершения криминальных деяний по мотивам самореализации до трансформации такой деятельности в преступный бизнес.

В третьей главе "Особенности расследования преступлений против информационной безопасности" рассмотрены вопросы построения модели расследования преступлений против информационной безопасности в условиях типичной следственной ситуации, а также тактические аспекты проведения отдельных следственных действий по уголовным делам данной категории.

Особенности противоправных деяний, совершаемых в сфере информационной безопасности, обуславливают использование качественно новых подходов к организации расследования и построению частной методики расследования преступлений. В основе такой методики лежит правовое обеспечение расследования и обусловленная ей информационная основа в виде криминалистической структуры преступлений, положения которой позволяют осуществить построение теоретико-прикладной модели расследования криминальных деяний в рассматриваемой сфере и разработать практические рекомендации по ее реализации.

Одной из предпосылок успешной борьбы с преступлениями против информационной безопасности является формирование качественного материала доследственной проверки, на основании которого возможно возбуждение уголовного дела, его быстрое расследование и направление в суд. При этом на первый план выходит работа оперативных подразделений по получению такого материала и его последующей реализации. В процессе выявления преступлений в данной сфере представляется целесообразным более широкое использование возможностей оперативно-розыскной деятельности по установлению лиц склонных к совершению подобных преступлений, их совершающих, а также мест концентрации этих лиц с целью обеспечения их оперативного прикрытия.

Практика борьбы с изучаемыми противоправными деяниями показывает, что следственные ситуации, складывающиеся при расследовании преступлений против информационной безопасности, могут быть классифицированы основе степени осведомленности органов уголовного преследования о субъекте преступления следующим образом: имеются данные, указывающие на признаки преступления, сведения о лице / лицах, причастных к его совершению, отсутствуют; имеются данные, указывающие на признаки преступления, сведения о лице / лицах, причастных к его совершению, неполные либо неточные; имеются данные, указывающие на признаки преступления, при этом установлено лицо, его совершившее, и его местонахождение. Важным свойством всех ситуаций является их повторяемость, что создает необходимые гносеологические предпосылки для предвидения их в будущем и использования при построении теоретико-прикладных моделей расследования в условиях типичной следственной ситуации.

Специфика расследования преступлений против информационной безопасности обуславливает необходимость применения специальных знаний в форме экспертного исследования и получения помощи сведущих лиц при проведении следственных действий. В то же время полученные данные свидетельствуют, что использование специалистов в ходе расследования имеет эпизодический характер и негативно сказывается на процессе установления истины. В силу этого, полагаем обоснованным развитие следственной практики по пути привлечения специалиста к участию в следственных действиях одновременно с самостоятельным овладением следователем (оперативным

работником) специальными знаниями в исследуемой сфере, что позволит более целенаправленно их использовать в ходе расследования, а также обеспечит непосредственное восприятие последствий совершенного преступления.

ЗАКЛЮЧЕНИЕ

На основании результатов диссертационного исследования представляется возможным сделать следующие выводы:

1. Анализ развития теоретико-правовых взглядов на проблему преступности в сфере информационной безопасности позволил расширить научные представления об исследуемом явлении, формах и методах борьбы с ним и на этой основе предложить качественно новые подходы, как к организации расследования противоправных деяний, так и к построению частной методики их расследования.

Содержание такой методики включает в себя: информационную основу расследования преступлений, состоящую из уголовно-правовой квалификации противоправных деяний и криминалистической структуры криминальных деяний данного вида, а также методическую основу расследования в форме теоретико-прикладных моделей расследования в условиях типичной следственной ситуации и рекомендаций по осуществлению отдельных следственных действий, направленных на реализацию ее положений. Использование этого подхода обусловлено специфичностью и новизной криминальных посягательств в рассматриваемой сфере, что требует формирования информационной основы расследования и включения в нее положений правовых норм, регламентирующих особенности квалификации и расследования преступлений [1; 16; 18].

2. Исследование правовых основ расследования преступлений против информационной безопасности позволило выявить правовые предпосылки и условия эффективной борьбы с ними, глубже понять систему общественных отношений, складывающихся в этой сфере, характер преступных действий, особенности квалификации преступлений, а также определить в законодательстве пробелы, которыми могут воспользоваться правонарушители для реализации своих преступных намерений и уклонения от ответственности.

Для повышения эффективности борьбы с преступлениями в сфере информационной безопасности представляется целесообразным совершенствование уголовного и административного законодательства. Кодекс об административных правонарушения следует дополнить следующими статьями: ст. 22.6.1 “Модификация компьютерной информации”, ст. 22.6.2 “Неправомерное завладение компьютерной информацией”.

В Уголовном кодексе следует внести изменения в статью 350 “Модификация компьютерной информации”, а также дополнить такими нормами: ст. 349^1 “Несанкционированный доступ к компьютерной информации”, ст. 350^1 “Модификация компьютерной информации”, 352^1 “Неправомерное завладение компьютерной информацией”.

Анализ практики расследования дает основание полагать, что данные изменения и дополнения удовлетворяют современным потребностям правоприменительной деятельности и будут способствовать эффективному решению задач уголовного процесса при расследовании и судебном рассмотрении уголовных дел в сфере информационной безопасности. Кроме того диссертантом доказана корреляционная связь между нормами права и эффективностью борьбы с преступлениями в рассматриваемой сфере, обусловленная их содержательным наполнением и своевременностью внесения изменений и дополнений [1; 4; 10].

3. Использование системно-структурного подхода при изучении такой категории, как "криминалистическая структура преступления", позволяет диссертанту сформировать понятие и раскрыть его содержание. Криминалистическая структура преступлений – это система криминалистически значимых сведений, детерминированная результатами взаимодействия преступника с окружающей средой, полученная в ходе анализа и обобщения следственной и судебной практики и выступающая основой для формирования рекомендаций по раскрытию и расследованию отдельных видов и групп преступлений.

Введение в научный оборот представленной дефиниции позволит реализовать потенциал системно-структурного подхода при изучении такого многогранного явления как преступление и предложить единый термин, раскрывающий его криминалистическую сущность [7; 9; 18].

4. Систематизация сведений о криминалистически значимых элементах структуры криминального деяния обуславливает возможность формирования новых подходов к разработке методики расследования преступлений отдельных видов и групп путем использования жесткой детерминированности между элементами системы преступной деятельности, что позволяет создать реальные предпосылки для реализации теоретико-прикладной модели расследования преступлений в условиях типичной следственной ситуации. Анализ практики расследования криминальных деяний против информационной безопасности позволил определить следующие наиболее значимые элементы криминалистической структуры: объекты-носители следов преступной деятельности; особенности обстановки реализации преступного замысла; способы совершения преступлений в сфере информационной безопасности; личность преступника.

Обобщение и систематизация сведений об указанных выше элементах криминалистической структуры преступлений против информационной безопасности позволили сформировать о них объективные научные представления, которые выступают основой для выдвижения версий, определения особенностей организации расследования, а также правильного выбора органом, ведущим уголовный процесс тактики проведения отдельных следственных действий.

Кроме того установлено, что указанные элементы криминалистической структуры образуют между собой закономерные связи, характер которых вы-

ражается в возможности установления способа совершения преступления в результате изучения обстановки криминального события и объектов-носителей следов противоправной деятельности, что является ключевым моментом, позволяющим выдвинуть версии относительно личности преступника и наметить направления розыскной работы и обнаружения следов преступного воздействия на компьютерную систему, применить соответствующие криминалистические приемы, методы и средства для расследования противоправного деяния [3; 5; 6; 9; 11; 14].

5. При расследовании преступлений против информационной безопасности целесообразно использование нового подхода к организации расследования путем формирования методического блока рекомендаций в форме теоретико-прикладных моделей расследования и рекомендаций по проведению следственных действий. При этом под теоретико-прикладной моделью расследования понимается мысленно представленная система действий, реализация которых направлена на оптимизацию процесса расследования криминальных деяний путем определения таких действий, их очередности и тактики осуществления.

Содержание ее раскрывается через систему действий, имеющих функционально-деятельностное предназначение для анализа исходной информации; определения сложившейся следственной ситуации; выдвижения общих и частных версий; определения направлений расследования в данной следственной ситуации; возбуждения уголовного дела; формирования перечня обстоятельств, подлежащих доказыванию; определения очередности и тактики проведения следственных действий и иных мероприятий, направленных на установление обстоятельств совершенного преступления. Содержательное наполнение теоретико-прикладных моделей расследования преступлений против информационной безопасности формируется с учетом типичной следственной ситуации. Отличительной особенностью теоретико-прикладной модели является возможность неоднократного применения, обусловленная ее нематериальным характером, что является существенным условием для ее использования в правоохранительной деятельности.

Анализ правоприменительной деятельности обуславливает необходимость формирования научно-практических рекомендаций проведения отдельных следственных действий, направленных на реализацию положений теоретико-прикладных моделей. В этой связи, представляются отвечающими потребностям правоприменительной деятельности сформированные рекомендации по проведению следственных действий при расследовании преступлений против информационной безопасности таких, как осмотр места происшествия, обыск, выемка, следственный эксперимент, допрос, назначение компьютерно-технических экспертиз [1; 2; 8; 12; 13; 15; 16; 17].

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Егоров Ю.А., Лепёхин А.Н. Тактические особенности проведения обыска по делам о преступлениях в сфере информационной безопасности // Вестн. Акад. МВД Респ. Беларусь. – 2003. – № 2. – С. 66 – 70.

2. Лепёхин А.Н. Эволюция способов преступления в сфере информационной безопасности // Вестн. Акад. МВД Респ. Беларусь. – 2004. – № 1. – С. 84 – 86.

3. Лепёхин А.Н. Правовые основы борьбы с преступлениями в сфере информационной безопасности // Вестн. Белгор. юрид. ин-та МВД России. – 2004. – № 3. – С. 52 – 57.

4. Лепёхин А.Н. Криминалистический анализ личности преступника по делам в сфере информационной безопасности // Проблемы правоохранительной деятельности: Международный научно-теоретический журнал № 1(1) – Белгород, 2005. – С. 77 – 82.

5. Лепёхин А.Н. К вопросу о криминалистической структуре преступления // Весці Нацыянальнай Акадэміі навук Беларусі, серыя гуманітарных навук, 2005. –№ 5/1. – С. 77 – 79.

6. Егоров Ю.А., Лепёхин А.Н. К вопросу об основных элементах криминалистической характеристики преступлений в сфере информационной безопасности // Закон и жизнь: Международный научно-практический правовой журнал. № 12 (169). – Кишинев, 2005. – С. 45 – 51.

7. Лепёхин А. Преступления против информационной безопасности: правовые аспекты // Судовы веснік. – 2006. – № 1. – С. 57 – 59.

8. Лепёхин А.Н. Противодействие преступности в сфере информационной безопасности // Проблемы криминалистики: Сб. науч. тр. / Под общ. ред. Г.Н. Мухина. – Минск: Акад. МВД Респ. Беларусь, 2003. – С. 136 – 139.

9. Лепёхин А.Н., Егоров Ю.А. Теоретические основы расследования и основные элементы криминалистической характеристики преступлений в сфере информационной безопасности // Сб. научных работ студентов высших учебных заведений Республики Беларусь «НИРС – 2004». В 2 ч.Ч. II. – Минск: ВЭВЭР, 2005. – С. 196 – 200.

10. Лепёхин А.Н. Исследование объектов-носителей следов преступной деятельности в сфере информационной безопасности // Проблемы криминалистики: сб. науч. тр. / отв. ред. д-р юрид. наук, проф. Г.Н. Мухин. – Минск: Акад. МВД Респ. Беларусь, 2005. – С. 75 – 82.

11. Лепехин А.Н. Актуальные вопросы наложения ареста на электронные почтовые отправления // Комплексная защита информации: Тез. докл. VII Междунар. конф., Раубичи, 25 – 27 февр. 2003 г. / Отв. ред. А.П. Леонов. – Минск: НАН Респ. Беларусь. Объед. ин-т проблем информатики, 2003. – С. 167 – 168.

12. Лепёхин А.Н. Следственный эксперимент по делам о преступлениях в сфере информационной безопасности: тактические аспекты // Южно-уральские криминалистические чтения: Сб. материалов науч.-практ. конф., посвя-

щенной 80-летию со дня рождения профессора Л.Л. Каневского / Под ред. И.А. Макаренко. – Уфа: РИО БашГУ, 2005., Выпуск 13. – С. 78 – 86.

13. Лепехин А.Н. К вопросу о личности преступника по делам о преступлениях в сфере информационной безопасности // Проблемы борьбы с преступностью и подготовки кадров для органов внутренних дел Республики Беларусь: Сб. материалов науч.-практ. конф., Минск, 28 янв. 2003 г. / Под общ. ред. И.И. Басецкого. – Минск: Акад. МВД Респ. Беларусь, 2003. – С. 79 – 81.

14. Лепехин А.Н., Егоров Ю.А. Тактика подготовки обыска по делам о преступлениях в сфере информационной безопасности // Проблемы борьбы с преступностью и подготовки кадров для органов внутренних дел Республики Беларусь: Сб. материалов науч.-практ. конф., Минск, 28 янв. 2003 г. / Под общ. ред. И.И. Басецкого. – Минск: Акад. МВД Респ. Беларусь, 2003. – С. 65 – 67.

15. Лепехин А.Н. Особенности обстановки совершения преступлений в сфере информационной безопасности // Юридическая наука и образование в Республике Беларусь на современном этапе: Материалы междунар. науч. конф., Гродно, 31 окт. 2003 г. / Отв. ред. Г.А. Зорин. – Гродно: ГрГУ, 2003. – С. 305 – 307.

16. Лепехин А.Н. Об использовании специальных знаний при расследовании преступлений в сфере информационной безопасности // Проблемы борьбы с преступностью и подготовки кадров для органов внутренних дел Республики Беларусь: Сб. материалов науч.-практ. конф., Минск, 30 янв. 2004 г. / Под общ. ред. И.И. Басецкого. – Минск: Акад. МВД Респ. Беларусь, 2004. – С. 138 – 139.

17. Лепехин А.Н., Егоров Ю.А. Особенности расследования преступлений в сфере информационной безопасности на первоначальном этапе // Комплексная защита информации: Сб. материалов VIII междунар. конф., Валдай (Россия), 23-26 марта 2004 г. / Отв. ред. А.П. Леонов. – Минск, 2004. – С. 184 – 187.

18. Лепехин А.Н. Особенности проведения осмотра места происшествия по делам о преступлениях в сфере информационной безопасности // Право Беларуси: истоки, традиции, современность: Материалы междунар. науч.-практ. конф., Новополоцк, 21 – 22 мая 2004 г.: В 2 ч. / Новополоцк: Полоц. гос. ун-т, 2004. – Ч. 2. – С. 189 – 191.

19. Лепёхин А.Н. Некоторые проблемы расследования преступлений против информационной безопасности и пути их разрешения // Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы безопасности. Выпуск VII: Сб. материалов междунар. науч.-практ. конф., Калининград, 24-25 окт. 2006 г. / Калининград: Калининградский юридический институт МВД России, 2006. – Ч. 1. – С. 62 – 69.

РЭЗЮМЭ

Лянёхін Аляксандр Мікалаевіч

КРЫМІНАЛІСТЫЧНАЕ ЗАБЕСПЯЧЭННЕ РАССЛЕДАВАННЯ ЗЛАЧЫНСТВАЎ СУПРАЦЬ ІНФАРМАЦЫЙНАЙ БЯСПЕКІ

Ключавыя словы: злачынствы супраць інфармацыйнай бяспекі, прававая аснова, крыміналістыная структура злачынства, асоба злачынцы, спосабы здзяйснення, мадэль расследавання.

Аб'ектам даследавання з'яўляюцца правазносіны, якія ўзнікаюць, развіваюцца і спыняюцца ў сувязі з дзейнасцю органаў крымінальнага праследавання па расследаванню злачынстваў супраць інфармацыйнай бяспекі. Прадмет даследавання складаюць заканамернасці здзяйснення злачынстваў супраць інфармацыйнай бяспекі, а таксама тэарэтычныя, прававыя і прыкладныя аспекты іх расследавання.

Мэтай даследавання з'яўляецца распрацоўка новых падыходаў да структуры прыватнай крыміналістычнай методыкі і выпрацоўка на падставе атрыманых тэарэтычных палажэнняў навукова-практычных рэкамендацый па расследаванню злачынстваў супраць інфармацыйнай бяспекі. У ходзе выканання дысертацыі выкарыстоўваліся агульнанавуковыя і спецыяльныя метады, вывучаліся архіўныя крымінальныя справы.

Навуковая навізна атрыманых у ходзе даследавання вынікаў вызначаецца наступным: сфарміраваны новы падыход да вызначэння структуры прыватнай крыміналістычнай методыкі, якая ўключае інфармацыйную і метадычную аснову расследавання злачынстваў супраць інфармацыйнай бяспекі, устаноўлена карэляцыйная сувязь паміж нормамі права і эфектыўнасцю барацьбы са злачынствамі ў разгледжанай сферы і сфармуліраваны канкрэтныя прапановы па іх удасканаленню; удакладнены існуючыя і распрацаваны новыя дэфініцыі; створана тэарэтыка-прыкладная мадэль расследавання злачынстваў супраць інфармацыйнай бяспекі і сфарміраваны практычныя рэкамендацыі па яе рэалізацыі.

Вынікі даследавання ўкаранены ў дзейнасць праваахоўчых органаў, заканатворчую практыку Нацыянальнага сходу Рэспублікі Беларусь, навучальны працэс Акадэміі МУС Рэспублікі Беларусь і Інстытута нацыянальнай бяспекі Рэспублікі Беларусь.

РЕЗЮМЕ

Лепёхин Александр Николаевич

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: преступления против информационной безопасности, правовая основа, криминалистическая структура преступления, личность преступника, способы совершения, модель расследования.

Объектом исследования являются правоотношения, которые возникают, развиваются и прекращаются в связи с деятельностью органов уголовного преследования по расследованию преступлений против информационной безопасности. Предмет исследования составляют закономерности совершения преступлений против информационной безопасности, а также теоретические, правовые и прикладные аспекты их расследования.

Целью исследования является разработка новых подходов к структуре частной криминалистической методики и выработка на основе полученных теоретических положений научно-практических рекомендаций по расследованию преступлений против информационной безопасности. В ходе выполнения диссертации использовались общенаучные и специальные методы, изучались архивные уголовные дела.

Научная новизна полученных в ходе исследования результатов определяется следующим: сформирован новый подход к определению структуры частной криминалистической методики, включающей информационную и методическую основу расследования преступлений; проанализировано содержание правовых основ расследования преступлений против информационной безопасности, установлена корреляционная связь между нормами права и эффективностью борьбы с преступлениями в рассматриваемой сфере и сформулированы конкретные предложения по их совершенствованию; уточнены существующие и разработаны новые дефиниции; создана теоретико-прикладная модель расследования преступлений против информационной безопасности и сформированы практические рекомендации по ее реализации.

Результаты исследования внедрены в деятельность правоохранительных органов, законотворческую практику Национального собрания Республики Беларусь, учебный процесс Академии МВД Республики Беларусь и Института национальной безопасности Республики Беларусь.

RESUME

Lepyokhin Alexandr Nikolayevich

CRIMINALISTIC SUPPORT OF INVESTIGATION OF CRIMES AGAINST INFORMATION SECURITY

Key words: crimes against information security, legal basis, criminalistic structure of crime, criminal personality, modi operandi, model of investigation.

The object of the thesis is social relations, which appear, develop and decease in connection with the activity of prosecuting agencies on investigation of crimes against information security. The subject of the thesis is objective laws of commission of crimes against information security, as well as theoretical, legal, and applied aspects of their investigation.

The purpose of the thesis is the development of new approaches to the structure of special criminalistic methodology and working out of scientific and practical recommendations for investigation of crimes against information security on the basis of theoretical results received. In the process of research general scientific and special methods have been used, archival criminal files have been studied.

Scientific novelty of the results received in the process of the research is the following: ne special criminalistic methodology, sis of criminal investigation, is f estigation of crimes against infor ction between legal norms and ef l and certain proposals of their p e specified and new ones are deve on of crimes against information s ns on its realization are formed.

The resul of law-enforcement agencies, legi Republic of Belarus, educational p l Affairs and the Institute of Nati