КАРАГАНДИНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РК
ИМЕНИ БАРИМБЕКА БЕЙСЕНОВА

УДК 343.98.068:007

На правах рукописи

НУГМАНОВА (ЗАВОТПАЕВА)
АЛИЯ ТЛЕУКУЛОВНА

Преступления в сфере высоких информационных технологий: теория и практика их расследования на первоначальном этапе

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

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук,
профессор
Исаев А. А.

Республика Казахстан
Караганда, 2007

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

МВД — Министерство внутренних дел
РК — Республика Казахстан
ЭВМ — электронно-вычислительная машина
УК — Уголовный кодекс
УПК — Уголовно-процессуальный кодекс
п. — пункт
ч. — часть
ст. — статья
ДВД — Департамент внутренних дел
УВД — Управление внутренних дел
КНАСОН — Комитет по надзору и аттестации в сфере образования и науки
МОиН — Министерство образования и науки
СССР — Союз советских социалистических республик
ООН — Организация объединенных наций
США — Соединенные штаты Америки
ФРГ — Федеративная Республика Германия
ОЗУ — оперативное запоминающее устройство
ЭВТ — электронно-вычислительная техника
CD-ROM — накопитель на оптических дисках
РФ — Российская Федерация
ЛЭС — линии электросвязи
ОРМ — оперативно-розыскные мероприятия
ФБР — Федеральное бюро расследований
СКТ — средства компьютерной техники
СВТ — средства вычислительной техники
ПК — персональный компьютер
ТОО — товарищество с ограниченной ответственностью
ЗАО — закрытое акционерное общество
БССР — Белорусская советская социалистическая республика
DISKCOPY — программа копирования дисков
ПЗУ — постоянное запоминающее устройство
ГРКЦ — Главный расчетно-кассовый центр
ЦБР — Центральный Банк России
ГУВД — городское управление внутренних дел
КБ — коммерческий банк
АО — акционерное общество
СОГ — следственно-оперативная группа
ОВД — органы внутренних дел
МНИ — машинные носители информации

ВВЕДЕНИЕ

Общая характеристика работы. В диссертации исследуются теоретические и прикладные вопросы расследования преступлений в сфере высоких информационных технологий, а также вопросы раскрытия преступлений данного вида.

Актуальность темы диссертационного исследования. На сегодняшний день Казахстан вступает на очередной этап научно-технической революции — становление информационного общества, основными чертами которого являются ускорение темпов развития техники, автоматизация обработки информации, создание новых интеллектуальных технологий, превращение информации в важнейший глобальный ресурс человечества. Перечисленные факторы ведут к кардинальному, многоуровневому изменению культурной, политической, правовой жизни, социальной среды. За последние годы многие государства в качестве приоритетной задачи выделили разработку и реализацию концепций и программ по переходу к информационному обществу. Поставленная Президентом Республики Казахстан цель — «… ускорить реализацию проекта “электронного правительства» и принятие Закона “О национальных реестрах идентификационных номеров”» [1] обуславливает создание нового информационного пространства и открывает совершенно новые, ранее неизвестные и недоступные возможности, которые коренным образом меняют представления о существовавших ранее технологиях получения и обработки информации, повышают эффективность функционирования различных организаций и учреждений, вхождение их в мировое информационное сообщество.

Информатизация современного общества привела к формированию новых видов преступлений с использованием устройств, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие информационные технологии. Остается актуальной проблема борьбы с организованной преступностью, которая, прибегая к услугам высококвалифицированных специалистов, стала все чаще использовать различные технические средства — от обычных персональных компьютеров и традиционных средств связи до сложных вычислительных систем и глобальных информационных сетей, в том числе и Интернет (International Network — международная система связи).

Учитывая специфику совершения преступлений в сфере высоких информационных технологий, следует отметить, что они чрезвычайно латентны (около 90 %). Это связано с тем, что указанные преступления имеют ряд отличительных особенностей. Во-первых, это высокая скрытность, сложность сбора улик по установленным фактам. Во-вторых, даже единичным преступлением наносится весьма высокий материальный ущерб. В-третьих, совершаются эти преступления высоко квалифицированными системными программистами, специалистами в области телекоммуникаций.

Особая актуальность вопросов защиты прав в отношении средств электронно-вычислительной техники, информационно-обрабатывающих технологий и

информации была отмечена и отечественным законодателем. Так, Законом РК «О национальной безопасности» от 26 июня 1998 г. было введено понятие «информационная безопасность» 2, а также Уголовный кодекс РК 1997 г. закрепил в ст. 227 состав преступления, предусматривающего ответственность за такого рода деяния. В связи с чем правоохранительные органы получили реальное средство борьбы с лицами, совершающими преступления в сфере высоких информационных технологий.

Вопросы, связанные с расследованием и раскрытием преступлений в сфере высоких информационных технологий, являются актуальными в теоретическом и практическом аспектах, что обусловлено рядом факторов.

В теории отечественной науки криминалистики отсутствуют исследования, раскрывающие понятие, содержание и сущность видов преступлений в сфере высоких информационных технологий, а также их классификацию.

Производство расследования преступлений в сфере высоких информационных технологий представляет собой для практических работников сложность в силу малоизученности этого явления. В результате проведенного исследования, опрос следователей и специалистов в области вычислительной техники показал, что только 14 % следователей работают на ЭВМ на уровне пользователя, 56 % не знают ничего о принципах работы ЭВМ, а о существовании тех или иных способов совершения преступлений в сфере высоких технологий знают всего 20 % респондентов. При этом 92 % из числа опрошенных программистов считают, что на современном уровне развития вычислительной техники без участия профессионала найти «спрятанную» в компьютере информацию без риска уничтожения очень сложно.

Подтверждением тому являются и результаты изучения 85 уголовных дел о преступлениях, связанных с информационными технологиями, при расследовании которых следователи использовали в основном традиционный арсенал следственных действий, без учета возможностей современных научно-технических достижений.

Опросы практических работников следствия и дознания свидетельствует о востребованности исследования криминалистических аспектов борьбы с преступлениями в сфере высоких информационных технологий (94 % опрошенных лиц).

Из указанного следует закономерный вывод, что важным условием эффективной организации борьбы с преступлениями в сфере высоких информационных технологий является знание специфики совершаемых преступлений, уяснение сущностных характеристик процессов, протекающих в соответствующей преступной среде.

При этом теоретическая и практическая значимость исследования обусловлена проводимой судебно-правовой реформой и объективной востребованностью научно обоснованного анализа вопросов криминалистического обеспечения борьбы с преступлениями в сфере высоких информационных технологий. Изложенные факторы в достаточной степени подтверждают обоснованность

выбора темы, актуальность направления научных изысканий, предопределяют теоретическую и практическую значимость темы исследования.

Цели и задачи исследования. Целью настоящего исследования является: определение методики расследования преступлений в сфере высоких информационных технологий на первоначальном этапе, раскрытие ее содержания, значения для защиты законных прав и интересов граждан и установления объективной истины в процессе расследования преступлений, а также разработка на данной основе криминалистических, уголовно-процессуальных и уголовно-правовых рекомендаций, направленных на совершенствование борьбы с преступлениями в сфере высоких информационных технологий.

Достижение названной цели было связано с необходимостью решения следующих задач:

– раскрыть сущность и содержание понятия преступления в сфере высоких информационных технологий;

– представить классификацию преступлений в сфере высоких информационных технологий;

– определить основные элементы криминалистической характеристики преступлений в сфере высоких информационных технологий;

– разработать алгоритм расследования и совокупность тактико-криминалистических средств производства следственных действий при расследовании преступлений в сфере высоких информационных технологий на первоначальном этапе;

– определить пути совершенствования борьбы с преступностью в сфере высоких информационных технологий;

– на основе теоретического, нормативного осмысления, анализа эмпирического материала выработать рекомендации, направленные на оптимизацию практики расследования преступлений в сфере высоких информационных технологий.

Объект и предмет исследования. ***Объектом*** данного исследования является преступная деятельность при совершении преступлений в сфере высоких информационных технологий и практика правоохранительных органов по предупреждению, раскрытию и расследованию этих преступлений.

Предметом исследования выступают нормы Конституции Республики Казахстан, уголовного права, уголовно-процессуального законодательства, других нормативных правовых актов Республики Казахстан, регламентирующие вопросы предупреждения, раскрытия и расследования преступлений в сфере высоких информационных технологий.

Кроме того, предметом изучения явились аналогичные нормы зарубежного права, имеющие значение для уголовно-процессуального законодательства, материалы следствия, дознания, прокуратуры, суда, экспертной деятельности по рассматриваемым вопросам.

Степень разработанности темы исследования. Теоретическую базу исследования составили труды таких ученых, как: А. Н. Ахпанов, А. Ф. Аубакиров,

Ю. М. Батурин, Д. И. Бедняков, Р. С. Белкин, И. Ш. Борчашвили, Л. В. Винницкий, А. Я. Гинзбург, Ю. Гульбин, Е. Г. Джакишев, А. М. Жодзишский, А. А. Исаев, М. Ч. Когамов, К. В. Ким, А. П. Кузьмин, Ю. Д. Лифшиц, Г. А. Мозговых, Б. М. Нургалиев, Р. А. Назмышев, С. С. Овчинский, Е. Т. Оспанов, Г. И. Поврезнюк, И. Л. Петрухин, В. Ю. Рогозин, Н. А. Селиванов, В. В. Степанов, М. С. Строгович, А. В. Сырбу, Б. Х. Толеубекова, И. Я. Фойницкий, А. А. Чувилев, А. Д. Шаймуханов, С. А. Шейфер, А. Ю. Шумилов, П. С. Элькинд, Р. Х. Якупов и других.

Научно-теоретическую основу выполненного исследования также образуют труды известных ученых в области теории государства и права, уголовно-процессуального, уголовного, административного, гражданского права, криминалистики, информатики и других отраслей права. Кроме того, использованы разработки ученых в области философии и социологии.

Методология и методика исследования. Методологическую базу исследования составили положения диалектико-материалистического метода, а также использование общенаучных и специальных методов научного исследования: аналогии, анализа, сравнения, синтеза, системно-структурного метода, исторического, сравнительно-правового, социологического, анкетирования и других методов.

Нормативной основой исследования являются: Конституция Республики Казахстан, Международные конвенции и договоры, конституционные законы, Уголовный кодекс Республики Казахстан, Уголовно-процессуальный кодекс Республики Казахстан, другие законы и иные нормативные правовые акты Республики Казахстан, а также нормативно-правовые акты зарубежных государств, относящиеся к теме исследования.

Эмпирическую базу составили результаты опроса 50 работников прокуратуры и 200 работников следствия и дознания, 60 специалистов и экспертов, а также изучение 300 уголовных дел, в процессе расследования которых использовалась компьютерная техника, возбужденных и законченных производством, приостановленных, прекращенных в период с 2000-2006 гг. дел. Средний стаж работы в должности указанных лиц составил 5 лет. Сбор эмпирического материала проводился на территориях Центрального, Восточного, Западного, Южного и Северного регионов Республики Казахстан.

Научная новизна диссертационного исследования. В криминалистической науке Республики Казахстан отсутствуют исследования, посвященные самостоятельному изучению проблемы расследования преступлений в сфере высоких информационных технологий, как в целом, так и на первоначальном этапе. В этой связи, научная новизна исследования заключается в том, что на монографическом уровне впервые осуществлено комплексное изучение методических вопросов расследования преступлений в сфере высоких информационных технологий на первоначальном этапе.

Диссертантом сформулированы новые теоретические положения, направленные на определение сущности и значения преступлений в сфере высоких информационных технологий, совершенствование законодательного регламен-

тирования, а также предложены практические рекомендации по оптимизации расследования преступлений в сфере высоких информационных технологий.

Основные положения, выносимые на защиту:

1. Реализация основных положений невозможна без определения специфики компьютерной информации, определения классификации, а также разработки определения понятия «преступления в сфере высоких информационных технологий» и его характерных особенностей.

2. Криминалистическая характеристика является такой криминалистической категорией, в рамках которой преступление изучается в пределах, обуславливающих возможность получения информации о преступлении и сведений об источниках такой информации. При этом элементный состав криминалистической характеристики в отношении отдельных видов преступлений может быть различным. Специфическими элементами криминалистической характеристики преступлений в сфере высоких информационных технологий являются:

а) характеристика личности преступника в сфере высоких информационных технологий, его типологические черты;

б) характеристика способов совершения преступления в сфере высоких информационных технологий;

в) характеристика орудий и средств, применяемых при совершении компьютерных преступлений;

г) характеристика обстановки, места и времени совершения преступлений.

3. Криминалистическая характеристика служит основанием криминалистического анализа процесса расследования преступления, включающего в себя типизацию версий и задач расследования, круг следственных действий и оперативно-розыскных мероприятий, направленных на решение данных задач, следственных ситуаций и выработку алгоритмов реализации тактических решений. На уровне элементного подхода к следственной ситуации выделяются основные критерии построения модели следственной ситуации применительно к расследуемому виду преступления. На основе указанной структуры определены и детально описаны типичные исходные следственные ситуации при расследовании преступлений в сфере высоких информационных технологий, программа проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий.

4. Статья 227 УК РК фактически предусматривает ответственность за совершение трех составов преступлений: 1) неправомерный доступ к охраняемой законом компьютерной информации; 2) создание, использование и распространение вредоносных программ для ЭВМ; 3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. На основе чего необходимо разработать методические рекомендации и схемы расследования первоначального этапа расследования отдельных видов преступлений в сфере высоких информационных технологий.

5. Проведенный анализ юридической литературы, посвященной общим вопросам тактики проведения отдельных следственных действий, показал на

необходимость исследования тактических особенностей проведения отдельных следственных действий при расследовании преступлений в сфере высоких информационных технологий: осмотра (включая несколько его разновидностей, а именно место происшествия, средств вычислительной техники, машинного носителя информации, машинного документа), обыска, выемки, допроса (подозреваемого, обвиняемого, свидетелей), следственного эксперимента, предъявления для опознания, назначение экспертиз.

6. С учетом особенностей данной категории деяний необходимо определить перечень основных обстоятельств (в нашему случае — 17 позиций), подлежащих доказыванию и установлению по делам о преступлениях в сфере высоких информационных технологий.

7. Определяя перспективы совершенствования борьбы с преступлениями в сфере высоких информационных технологий, предлагается внести дополнение в ч. 11 ст. 126 УПК РК «Закрепление доказательств» после слов «киносъемка, фотосъемка» словами «программные средства, использующих технологию оперирования информацией» и далее по тексту; а также после слов «с приведением технических характеристик использованных научно-технических средств...» словами «при применении программных средств, использующих технологию оперирования информацией, в протоколе указываются: наименование продукта, версия, код продукта, операционная система в которой используется программное средство»

В связи со спецификой данного вида преступлений, также хотелось бы внести дополнение и в уголовное законодательство. Так, ч. 1 ст. 54 УК РК «Обстоятельства, отягчающие уголовную ответственность и наказание» дополнить п. «р», изложив его в следующей редакции: «р) совершение преступления с использованием высокоточного оборудования, устройств и программных средств, использующих технологию оперирования информацией».

Теоретическая и практическая значимость результатов исследования определяется тем, что в ходе исследования раскрываются теоретические основы построения методики расследования преступлений в сфере высоких информационных технологий и методика расследования преступлений в сфере высоких информационных технологий на первоначальном этапе.

Кроме того, содержащиеся в диссертации выводы и предложения могут быть использованы: в научных исследованиях, направленных на развитие и углубление теории уголовно-процессуального права и криминалистики; в нормотворческом процессе при регламентации положений о преступлениях в сфере высоких информационных технологий; в правоприменительной деятельности органов уголовного судопроизводства при разрешении вопросов, связанных с расследованием преступлений в сфере высоких информационных технологий; в учебном процессе высших и специальных заведений юридического профиля, а также в системе первоначальной подготовки, повышения квалификации и переподготовки при изучении соответствующих тем.

Апробация и внедрение результатов исследования. Результаты проведенного исследования и сформулированные на их основе выводы, предложения

и рекомендации были обсуждены на кафедре криминалистики Карагандинского юридического института МВД РК имени Баримбека Бейсенова.

Концептуальные положения докладывались диссертантом на межвузовских, республиканских и международных научно-практических конференциях. Автором опубликовано девять научных статей, в которых излагаются основные результаты проведенного исследования.

Положения диссертационного исследования нашли применение в практической деятельности Управления криминальной полиции ДВД по Карагандинской области, следственных подразделений УВД и Прокуратуры г. Темиртау при расследовании преступлений данной категории, а также внедрены в учебный процесс при проведении занятий на факультете очного и заочного обучения Карагандинского юридического института МВД РК имени Б. Бейсенова и в Карагандинском государственном университете имени Е. А. Букетова.

Структура и объем диссертационного исследования. Структура определяется поставленными целями, задачами и логикой исследования. Работа состоит из введения, трех разделов, включающих четыре подраздела, заключения, списка использованных источников и приложений. Диссертация соответствует требованиям, предъявляемым КНАСОН МОиН Республики Казахстан к оформлению диссертационных работ, а ее объем составляет 163 листа текста компьютерного набора (приложения в указанный объем диссертации не входят).

1 ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Понятие и значение преступлений в сфере высоких информационных технологий. Проблемы уголовно-правовой квалификации

До недавнего времени считалось, что совершение преступлений, с использованием высоких информационных технологий — явление, присущее только зарубежным странам, и по причине слабой компьютеризации нашего общества, т. е. недостаточного внедрения в производственные и общественные отношения информационных технологий, отсутствует вообще. Именно это обстоятельство и привело к отсутствию сколько-нибудь серьезных научных исследований этой проблемы.

Компьютерно-информационные технологии функционируют относительно давно, и их развитие происходит огромными темпами, что связано с большой заинтересованностью в этом широких слоев населения. Преступления, связанные с использованием компьютерной техники, — это лишь специализированная часть преступной деятельности в информационной сфере [3, с. 50]. К данной категории относятся и преступления, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. В течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово-коммерческой деятельности появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики. Первое преступление подобного типа в бывшем СССР было зарегистрировано в 1979 г. в городе Вильнюсе. Тогда ущерб государству составил около 80 тысяч рублей. Этот случай явился определенной отправной точкой в развитии и исследовании нового вида преступлений.

Только в последние годы появились работы по проблемам борьбы с компьютерной преступностью, в которых рассматриваются в основном уголовно-правовые и криминологические аспекты этого явления. Как нередко случалось уже ранее, например, ситуация с наркоманией или с организованной преступностью, борьба с этим социально опасным явлением началась лишь после того, как материальные потери от этого вида преступлений достигли существенных размеров и стали резко выделяться на общем фоне потерь от обычных видов общеуголовной преступности.

Постепенно на наших глазах возникла информационная индустрия, чья самостоятельность и перспектива развития целиком и полностью зависели от точного регулирования правоотношений, возникающих при формировании и использовании информационных ресурсов. «Информационная революция» застигла страну в сложный экономический и политический период и потребовала срочного регулирования возникающих на ее пути проблем. Между тем, как известно, правовые механизмы могут быть включены и становятся эффективны-

ми лишь тогда, когда общественные отношения, подлежащие регулированию, в достаточной мере стабилизировались.

Для того чтобы четко определить суть проблемы, для любой науки вполне логичен подход, когда все исследователи конкретной предметной области организуют свое общение на основе единообразно понимаемых терминов и пытаются обеспечить некую стабильность понятийно-терминологического аппарата.

Отечественные и зарубежные издания и средства массовой информации последних лет наводнены различными понятиями, обозначающими те или иные новые проявления криминального характера в информационной области. При наличии довольно зримых контуров такого социально-правового феномена, каковым выступают преступления в глобальных компьютерных сетях, в теории до сих пор отсутствует его общепринятая правовая дефиниция. В литературе можно встретить целый ряд понятий («компьютерное преступление», «преступление в сфере высоких технологий», «коммуникационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «информационные преступления», «кибербандитизм», «сетевое преступление»), в основном подразумевающих одни и те же виды преступной деятельности. Зарубежными исследователями чаще используются такие понятия, как high-tech crime, cyber crime, network crime, которые соответственно переводятся как «преступления в сфере высоких технологий», «киберпреступления», «преступления в компьютерных сетях». Преступников именуют «хакеры», «кракеры», «киберпанки», «бандиты на информационных супермагистралях».

Так, А. В. Дулов к компьютерным преступлениям относит «различные преступления, совершаемые с помощью компьютеров, с нарушением их деятельности» [4, с. 3]. Нам кажется, подобное определение является довольно широким и содержащим существенную неточность: результатом компьютерного преступления не обязательно должно быть нарушение деятельности самих компьютеров. Общественно-опасные последствия могут наступать и при нормальном функционировании программно-аппаратных средств компьютера при условии неверных исходных данных, при ошибках оператора или программиста, при кражах машинного времени, неправомерном доступе и т. д.

Н. А. Селиванов относит к компьютерным преступлениям, преступления, предметом которых является компьютерная информация, либо средством совершения которых выступает электронно-вычислительная техника, используемая с целью совершения противоправного посягательства на иной объект [5, с. 37]. Опровергая данную точку зрения, В. В. Крылов [6, с. 4] считает, что подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя не оправдывает и поэтому нецелесообразно принимать термин «компьютерные преступления» за основу для наименования в криминалистике всей совокупности преступлений в области информационных отношений. Компьютер, по его мнению, является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением кон-

фиденциальной документированной информации. В. В. Крылов предлагает рассматривать в качестве базового понятия «информационные преступления», исходя из того, что сложившаяся система правоотношений в области информационной деятельности позволяет абстрагироваться от конкретных технических средств. Он делает вывод, что преступления в области компьютерной информации, выделенные в отдельную главу УК, являются частью информационных преступлений, объединенных общим инструментом обработки информации — компьютером.

Ю. М. Батурин подразделяет объекты компьютерных атак на три категории [7, с. 9]: сами компьютеры, объекты, которые могут быть атакованы с помощью компьютера как инструмента, объекты, для которых компьютер является окружением. Представляется обоснованным не включать в состав объектов компьютерных преступлений первую категорию по данной классификации в случаях, когда компьютеры являются не более чем имуществом, абсолютно равнозначным любым другим материальным вещам, и не подлежат выделению в отдельную правовую категорию единственно по признаку их наименования.

Классической точки зрения о том, что рамки компьютерных преступлений можно ограничить использованием ЭВМ в качестве инструмента (орудия) и предмета посягательства, придерживается и Н. Ф. Ахраменка. При этом указывает, что сам компьютер не может быть рассмотрен как предмет компьютерных преступлений, так как «предметом посягательств при их совершении является отнюдь не техника как таковая (ей ущерб, как правило, не наносится), а информация, хранимая, обрабатываемая или передаваемая этой техникой. Определяя объект компьютерных посягательств, мы исходим из того, что преступления такого рода с гораздо большим основанием следует отнести к информационным» [8, с. 23]. На наш взгляд, предмет компьютерных преступлений следует еще больше расширить: помимо информации включить еще нормальное функционирование вычислительной техники и течение информационных процессов.

Несомненно, данный перечень мнений не является исчерпывающим [6; 9; 10], однако важно другое: необходимо различать преступления в сфере высоких информационных технологий и так называемые компьютерные преступления. К сожалению, последний термин настолько прочно вошел в обиход научных и практических работников, как в Казахстане, так и за рубежом, что стал уже традиционным, и некоторые авторы полагают, что вряд ли стоит его менять, «поскольку многие названия со временем приобретают условный характер» [11, с. 21].

Различие в терминологии указывает не только на обеспокоенность общества новой угрозой, но и на отсутствие полного понимания сути этой угрозы. Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а, следовательно, и негативные последствия.

Следует отметить, что общепризнанного определения преступления, совершаемого с использованием или в отношении средств вычислительной техники, компьютерной информации, программного обеспечения, на сегодняшний

день не имеется, вообще, а уголовное право иностранных государств охватывает этим понятием различные по своему характеру и степени общественной опасности виды противоправных деяний.

Так, ООН, признавая указанные преступления глобальной международной проблемой в международном обозрении деятельности криминальной полиции «руководство по предотвращению и контролю над преступлениями, совершенными с использованием компьютеров», отмечает, что: «… законодательство и судебная система не успевают за развитием технического прогресса. Только незначительное количество государств имеет адекватное законодательство в указанной сфере, но и они не лишены правовых и правоприменительных недостатков» [12]. Наиболее распространенное определение — «преступление, совершенное с использованием компьютерной техники или направленное против безопасности компьютерной информации» [13, с. 465] — не отвечает потребностям науки и практики сегодняшнего дня и нуждается в уточнении.

К вопросу криминализации правонарушений в сфере высоких информационных технологий сегодня в мире существует три подхода [14, с. 13].

Первый заключается в отнесении к преступлениям несанкционированного доступа в защищенные компьютерные системы, заражения вирусами, противоправного использования компьютерных систем и информации. Он характерен для таких стран, как Норвегия, Сингапур, Словакия, Филиппины, Южная Корея.

Второй подход заключается в признании компьютерными преступлениями лишь тех деяний, которые связаны с причинением ущерба имуществу и электронной обработке информации (Австрия, Дания, Швеция, Швейцария, Япония). Например, в законодательстве Австрии, Дании, предусматривается уголовная ответственность за неправомочное вмешательство в функционирование информационно-вычислительных систем [15; 16].

Третий подход характерен для стран с высоким уровнем компьютеризации (США, Великобритания, Франция, Германия, Нидерланды) и развитой правовой базой. Он состоит в криминализации деяний, связанных не только с имущественным ущербом, но и с нарушением прав личности, с угрозой национальной безопасности и т. д. [17]. Так, из содержания норм уголовного права Великобритании следует, что его санкции применяются к «злоумышленникам, причинившим с помощью ЭВМ ущерб или использовавшим информацию в своих целях» [18, с. 14]. В 80-е годы системой уголовной юстиции ФРГ был предложен целый ряд уголовно-правовых определений исследуемой категории противоправных деяний. Уголовная полиция этой страны к преступлениям в сфере высоких технологий относит «все противоправные действия, при которых электронная обработка информации является орудием их совершения и(или) их объектом» [19, с. 13].

Следует отметить, что подобные преступления все чаще совершаются сотрудниками фирмы, банка или другого учреждения, которым в конечном итоге и наноситься ущерб. Например, в США компьютерные преступления, совершенные служащими, составляют 70-80 % ежегодного ущерба, связанного с

компьютерами. В Казахстане тоже существует такая тенденция. Так, в 2000 г. в Лондоне были арестованы О. Зезов и И. Яримак (граждане Казахстана) по обвинению в неавторизированном компьютерном проникновении, заговоре, нанесении вреда коммерции путем вымогательства и попытке нанесения вреда путем вымогательства с использованием корпоративной информации компании Bloomberg LP. Сумма шантажа составляла 200 тысяч долларов. Они были арестованы в аэропорту в момент передачи денег. Примечательно то, что, работая в компании, производящей базы данных для Bloomberg LP, они воспользовались полученной в ходе этого информацией для достижения своих преступных целей. Суд над ними состоялся лишь летом 2002 г., исходя из сложности доказывания такого преступления. В США, где проходило судебное разбирательство, максимальный срок наказания по совокупности за эти преступления составляет 28 лет [20].

Для того чтобы понять, что же представляет собой «охраняемая законом компьютерная информация», мы приведем краткий перечень некоторых видов информации, охраняемых законодательством Республики Казахстан, которые одновременно подлежат защите — государственные секреты; служебная и коммерческая тайна; банковская тайна; нераскрытая информация; личная и семейная тайны, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; тайна усыновления (удочерения) ребенка; адвокатская тайна; тайна пенсионных накоплений получателя [21, с. 5].

При этом информация — это сведения или данные, объективно отражающие различные стороны и элементы окружающего мира и деятельности человека на определенном этапе развития общества, представляющие для него какой-либо интерес, и материализованные в форме, удобной для использования, передачи, хранения и(или) обработки (преобразования) человеком или автоматизированными средствами [22, с. 82].

«Охраняемая законом компьютерная информация», как вид информации, представляет собой сведения, зафиксированные на машинном, магнитном носителе, представленные в форме набора состояний элементов ЭВМ, иных электронных средств обработки, хранения и передачи информации [23, с. 45].

Компьютерная информация имеет специфику, которую можно свести к следующему:

1) данная информация, как правило, очень объемна и быстро обрабатываема;

2) эта информация очень легко и, как правило, бесследно уничтожаема. Для уничтожения компьютерной информации, равной 500 страницам текста необходимы два нажатия клавиши клавиатуры, — через секунду вся она будет стерта. В то время как для сжигания 500 страниц машинописного или рукописного текста необходимы специальные условия и значительный промежуток времени;

3) компьютерная информация обезличена, т. е. между ней и лицом, которому она принадлежит, нет жесткой связи;

4) данный вид информации может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и др.), в самой ЭВМ (оперативной памяти — ОЗУ);

5) рассматриваемый вид информации может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВТ при наличии соответствующих периферийных устройств чтения машинных носителей информации (дисководы, устройства чтения лазерных дисков (CD-ROM), стримеры, устройства чтения цифровых видеодисков и др.);

6) эта информация легко передается по телекоммуникационным каналам связи компьютерных сетей, причем практически любой объем информации можно передать на любое расстояние [24, с. 208].

Компьютерную информацию можно классифицировать по:

– ее носителям: зафиксированная на магнитной ленте, дискетах (Floppy Disk), лазерных дисках, на жестком диске ЭВМ (Hard Disk), в памяти ЭВМ, системы ЭВМ или сети;

– типу информации — текстовая, числовая, графическая и др.;

– местонахождению информации — описание места расположения на временном или постоянном носителе и указание типа носителя;

– наименованию файла — символьное описание названия;

– размеру (объему) хранимой информации (количество страниц, абзацев, строк, слов, символов или байт);

– времени создания, времени изменения;

– атрибутам информации (архивная, скрытая, системная, только для чтения и др.).

К факультативным свойствам относятся: тема, автор, создавший или изменивший информацию; группа, в которую включен данный файл, ключевые слова, заметки автора или редактора. Возможны классификации и по другим основаниям.

По свидетельству специалистов, наиболее привлекательным сектором экономики практически любой страны является ее кредитно-финансовая система. Наиболее распространенным в этой области являются преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей. В России, например, только за 1 год было выявлено 15 подобных преступлений, в ходе расследования которых были установлены факты незаконного перевода 6,3 млрд. рублей [25]. В целом, в Российской Федерации в настоящий момент завершено производством около 100 уголовных дел, предусмотренных главой 28 Уголовного кодекса РФ. В Казахстане таковых дел единицы.

Компьютерная техника и средства коммуникаций на территории Республики Казахстан используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение машинного времени, а также денежных средств посредством электронной транзакции — вот далеко не полный перечень преступлений, с которыми вынужде-

ны бороться правоохранительные органы США, Канады, стран Европы и т. д.), а в большей степени как средства преступной деятельности. Причина — высокая латентность данного вида преступлений и слабо развитые, а иногда даже отсутствующие компьютерно-информационные сети. За рубежом, например, активно борются с проблемой латентности. Так, по данным Института компьютерной безопасности США (Computer Security Institute, CSI) из Сан-Франциско число компаний, сообщавших о компьютерных преступлениях в отношении той или иной их формы, выросло с 1998 г. по 2001 г. почти вдвое — с 17 % до 32 % [26].

Еще одна из причин роста таких преступлений в Казахстане — это разрыв в уровнях развития информационного общества по сравнению с Западом, порождающий иногда абсурдные ситуации, нестыковки моральных, правовых стандартов и норм. Создаются условия для соблазна, искушения воспользоваться более удобной и дешевой формой обеспечения информацией. Взять, например, проблему сохранения интеллектуальной собственности. Лицензионные программы стоят очень дорого для массового потребителя и нет моральных преград пользоваться «взломанными» программами, которые во много раз дешевле [27].

Как показывает практика, буквально единицы уголовных дел, возбужденных на территории стран бывшего Советского Союза, по сравнению с западными странами, связаны с незаконным доступом к охраняемой законом компьютерной информации, тогда как в большем количестве дел электронная информация фигурирует в качестве доказательств. Как отмечает В. Б. Крылов, правоохранительным органам становится известно не более 5-10 % совершенных компьютерных преступлений [28, с. 17]. Это связано с тем, что хищение информации долгое время может оставаться незамеченным, поскольку зачастую данные просто копируются. Жертвы компьютерной преступности (большинство из них частные предприниматели) проявляют нежелание контактировать с правоохранительными органами, опасаясь распространения среди вкладчиков и акционеров мнения о собственной халатности и ненадежной работе своей фирмы, что может инициировать отток финансов и последующее банкротство [29, с. 70]. Например, в Англии преступникам было выплачено 400 миллионов фунтов стерлингов в качестве отступного за обещание «не поднимать шума». Преступники осуществили электронное проникновение в ряд банков, брокерских контор и инвестиционных компаний Лондона и Нью-Йорка, установив там программы — вирусы, активизирующиеся по желанию преступников. Банки предпочли удовлетворить требования вымогателей, поскольку огласка случаев электронного взлома могла бы поколебать уверенность клиентов в безопасности банковских систем [30].

Если же в России одним из первых наиболее крупных компьютерных преступлений считается уголовное дело о хищении 125,5 тыс. долларов США и подготовке к хищению еще свыше 500 тыс. долларов во Внешэкономбанке СССР в 1991 г., то в Казахстане первое наиболее крупное преступление с использованием компьютерных технологий имело место в 1994 г. Тогда это было

первое уголовное дело против бывшего оператора Алатауского филиала КРАМС-банка г. Алматы Э. Р. Ордабаева, который путем использования ключевой шифровальной дискеты осуществил две фиктивные бухгалтерские проводки на сумму 6 млн. 795 тыс. тенге на счет малого предприятия «Анжелика» [31, с. 35].

Одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет. В настоящее время Интернет, использующий в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками, объединяющую около 30000 мелких локальных сетей и более 30 миллионов пользователей, число которых постоянно растет. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных минипроцессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам Интернет позволяет передавать не только аудио-, но и видеоинформацию, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, — возможность осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. Кроме того, существует проблема распространения в сети информации порнографического характера, которая, согласно ст. 273 Уголовного кодекса Республики Казахстан, является уголовно-наказуемым деянием.

Следует отметить, что понятие «компьютерных» или же «информационных» преступлений базируется исключительно на действующем уголовном законодательстве в этой области. Действительно, в России, например, глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации» предусматривает три состава преступлений — ст. ст. 272-274, в Республике Казахстан в главе 7 «Преступления в сфере экономической деятельности» — один состав преступлений — ст. 227 Уголовного кодекса РК. Название соответствующей главы в Уголовном кодексе РФ некоторые российские ученые связывают

с тем, что в формулировании соответствующих составов преступлений законодателем акцент был сделан на защиту именно самой компьютерной информации, хотя и признают, что название главы является в известной мере условным. В этом аспекте интересен подход законодателя Республики Беларусь, где в Уголовном кодексе [32] рассматриваемые преступления сгруппированы в разделе XII «Преступления против информационной безопасности» по признаку родового объекта посягательств — нормального течения информационных процессов, самой информации, путей ее передачи или способов обработки. Кроме того, компьютерным преступлением, в соответствии с данной выше классификацией, является предусмотренное ст. 212 «Хищение путем использования компьютерной техники». В последнем случае следует учитывать такую позицию законодателя, что использование компьютерной техники, как квалифицирующего признака при хищении, свидетельствует о повышенной общественной опасности таких действий. Родовым объектом вышеназванных преступлений являются многочисленные общественные отношения: обеспечивающие нормальный порядок управления, в области предпринимательства и иной хозяйственной деятельности, отношения собственности, общественной безопасности, причем в большинстве случаев посягательство касается сразу группы этих отношений в совокупности [33, с. 166].

Вместе с тем в ходе проведенного нами анализа действующего в Казахстане уголовного законодательства было установлено, что при совершении ряда других преступлений могут использоваться высокие технологии, и как показывают приведенные выше примеры различных тенденций развития подобных преступлений, используются они преступниками довольно эффективно. Приведем перечень некоторых действий преступников, использующих высокие технологии, и соответствующие им составы преступлений, предусмотренных в законодательстве РК:

1. Распространение через каналы сети Интернет и местных локальных сетей:

– заведомо ложных сведений, порочащих честь и достоинство лица или подрывающих его репутацию — ст. 129 УК РК «Клевета»;

– информации, связанной с унижением чести и достоинства лица, выраженной в неприличной форме — ст. 130 УК РК «Оскорбление»;

– сведений о частной жизни лиц, составляющих их личную или семейную тайну — ст. 142 УК РК «Нарушение неприкосновенности частной жизни»; тайну переписки, телефонных переговоров, почтовых, телеграфных или других сообщений — ст. 143 УК РК «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;

– информации, призывающей к развязыванию агрессивной войны — ст. 157 УК РК «Пропаганда и публичные призывы к развязыванию агрессивной войны»; к насильственному изменению государственного строя — ст. 170 УК РК «Призывы к насильственному свержению или изменению конституционного строя либо насильственному нарушению единства территории Республики Ка-

захстан», составляющей государственную тайну — ст. 172 УК РК «Разглашение государственной тайны» и т. п.;

– информации порнографического характера — ст. 273 УК РК «Незаконное распространение порнографических материалов и предметов».

2. Мошенничество в сфере использования азартных игр (казино, лотереи и тотализаторы), организации финансовых пирамид, фиктивных брачных контор и фирм по оказанию несуществующих услуг — ст. 177 УК РК «Мошенничество».

3. Получение вознаграждения за неразглашение сведений, полученных в ходе несанкционированного доступа к информации, составляющей коммерческую или банковскую тайну, — ст. 181 УК РК «Вымогательство», ст. 200 УК РК «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну».

4. Незаконное копирование и продажа программных продуктов, находящихся на серверах компаний, которые являются владельцами этих программ, с присвоением их авторства другим лицом либо компанией — ст. 184 УК РК «Нарушение прав интеллектуальной собственности», а также использование преступником логотипа или наименования товара другой фирмы — ст. 199 УК РК «Незаконное использование товарного знака».

5. Изготовление с использованием средств компьютерной техники поддельных денежных знаков и документов — ст. 206 УК РК «Изготовление или сбыт поддельных денег или ценных бумаг», ст. 207 «Изготовление или сбыт поддельных платежных карточек и иных платежных и расчетных документов», ст. 208 УК РК «Подделка и использование марок акцизного сбора» и т. п.

Таким образом, уголовная ответственность за использование высоких технологий для совершения преступлений охватывает довольно большой перечень общественных отношений, гораздо обширнее, на наш взгляд, чем отношения в области компьютерной информации.

По нашему мнению, различие между компьютерными преступлениями и преступлениями в сфере высоких информационных технологий следует проводить по объекту преступного посягательства. Если таковым выступают, допустим, отношения собственности, то деяние подлежит квалификации по соответствующей статье главы 6 УК РК, если объектом являются отношения по защите конституционных прав и свобод человека и гражданина, то деяние квалифицируется по соответствующей статье главы 3 УК РК и т. п. И только если таковым выступают отношения в сфере нормального оборота компьютерной информации, то деяние подлежит квалификации в соответствии со ст. ст. 172, 200, 227 УК РК. Таким образом, понятие компьютерных преступлений гораздо уже понятия преступлений в сфере компьютерной информации и охватывает все преступления, способом совершения которых является неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, нарушение правил эксплуатации ЭВМ, их системы или сети. Соответственно к преступлениям в сфере компьютерной ин-

формации относятся лишь составы, предусмотренные ст. ст. 172, 200, 227 УК РК.

Н наш взгляд, компьютерная техника во всех вышеперечисленных деяниях может быть использована как орудие преступления, однако наряду с нею возможно применение и других технических средств, то есть условие ее использования не является существенным для квалификации деяний по данным статьям, следовательно, компьютерными их назвать нельзя. В том же случае, если наряду с действиями, предусмотренными составами вышеназванных статей, правонарушитель допускает использование ЭВМ или противоправные действия в отношении информации, компьютерного оборудования и т. д., то содеянное следует квалифицировать по совокупности с нормами УК РК.

Как справедливо отмечает В. Н. Черкасов, компьютерное мошенничество, компьютерный саботаж, компьютерный шпионаж и т. п. остаются теми же мошенничеством, саботажем и шпионажем, лишь совершенными с использованием компьютеров, как неких технических средств [34, с. 5]. Своеобразным подтверждением этому можно считать мнение Е. Р. Россинской и Л. И. Усова, которые отмечают, что «дефиниция “компьютерные преступления” должна употребляться не в уголовно-правовом аспекте, где это затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования» [11, с. 22]. Высказывание относительно ненужности уголовно-правовой квалификации довольно спорно, так как довольно часто именно способ совершения преступления влияет на квалификацию деяния и, соответственно, меру наказания (например, кража, мошенничество, грабеж, разбой).

Подводя итог изложенному, следует отметить, что составы преступлений в сфере высоких информационных технологий объединяет единый родовой объект [35; 36; 37; 38]. При этом под объектом преступления понимается охраняемое уголовным законом общественное отношение, которому общественно-опасное деяние причиняет вред либо ставит под угрозу причинения такого вреда [39, с. 184].

При этом следует согласиться с мнением Н. В. Ветрова, который под родовым объектом данных преступлений понимает «общественные отношения в сфере обеспечения безопасности использования автоматизированных систем обработки данных, нормальных прав и интересов лиц, общества и государства, активно пользующихся электронно-вычислительной техникой» [40, с. 183].

Обобщая вышесказанное, можно выделить следующие характерные особенности преступлений в сфере высоких информационных технологий:

– неоднородность объекта посягательства;

– выступление компьютерной информации, как в качестве объекта, так и в качестве средства преступления;

– многообразие предметов и средств преступного посягательства;

– выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

Объективная сторона выражается в совершении ряда действий, которые можно классифицировать как:

– физические злоупотребления, которые включают в себя: разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях;

– операционные злоупотребления, представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств;

– программные злоупотребления, которые включают в себя: различные способы изменения системы математического обеспечения («логическая бомба» — введение в программу компьютера команды проделать в определенный момент какое-либо несанкционированное действие; «троянский конь» — включение в обычную программу своего задания);

– электронные злоупотребления, которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Очевидно, что частная методика расследования подобных преступлений не будет являться основной, предпочтение будет отдано специальным методикам расследования, построенным не по видам преступлений, а по другим основаниям. Анализ вышеизложенного позволяет указать в качестве оснований для выделения частной специальной методики расследования преступлений в рассматриваемой области преступную сферу использования информации в электронном виде. Кроме того, к основаниям могут быть отнесены и отдельные элементы криминалистической характеристики подобных преступлений, такие как объект посягательства, орудия и средства совершения этих преступлений, в качестве которых выступают устройства сбора, хранения и обработки информации, а также способы их совершения. Наряду с этим в качестве основания для выделения частной специальной методики, выступает и характер специальных знаний, используемых при расследовании подобных преступлений, которые, как справедливо отмечает отечественный ученый А. А. Исаев, используются при квалификации преступлений при установлении элементов состава преступлений [41, с. 24]. Так, путем привлечения специальных научных знаний в ходе расследования таких преступлений возможно установление предмета преступления, который в обобщенном виде для всей категории рассматриваемого вида преступлений представляет собой информацию в электронном виде и созданные на основе ее предметы реального мира или же совершенные в соответствии с ней какие-либо преступные деяния.

В результате анализа приведенных позиций и точек зрения можно определить данный вид преступлений как преступления в сфере высоких информационных технологий, под которыми понимается совершение противоправных деяний в области информационных отношений, осуществляемых посредством высокоточного оборудования, устройств и программных средств, использующих технологию оперирования информацией. Данный термин наиболее точно определяет преступления в рассматриваемой нами области. Расследование пре-

ступлений, совершенных с использованием средств компьютерных технологий, в таком случае будет являться составной частью расследования преступлений в сфере высоких информационных технологий.

Учитывая, что использование высокоточного оборудования и устройств, использующих технологию оперирования информацией, при совершении различного вида преступлений, свидетельствует о повышенной общественной опасности таких действий, а также то, что уголовно-правовое законодательство не в состоянии оперативно квалифицировать стремительное развитие всех видов и способов совершения указанной категории преступлений, предлагаем, дополнить ч. 1 ст. 54 УК РК «Обстоятельства, отягчающие уголовную ответственность и наказание» п. «р», изложив его в следующей редакции: «р) совершение преступления с использованием высокоточного оборудования, устройств и программных средств, использующих технологию оперирования информацией».

После детального рассмотрения основных компонентов, представляющих в совокупности содержание понятия преступлений в сфере высоких информационных технологий, можно перейти к рассмотрению вопросов, касающихся классификации преступлений в сфере высоких информационных технологий и исследованию основных элементов криминалистической характеристики.

1.2 Современное состояние и перспективы борьбы с преступлениями в сфере высоких информационных технологий и их классификация

На сегодняшний день проблема борьбы с международной преступностью в сфере высоких информационных технологий приобрела небывалую остроту. Стремительное развитие компьютерной техники и международных сетей как неотъемлемой части современной международной финансовой и банковской деятельности, а также таких сфер как производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации, создало предпосылки, в немалой степени облегчающие совершение преступных деяний как внутри страны, так и на международном уровне.

В современном компьютеризованном обществе почти все виды преступлений могут совершаться с помощью имеющейся компьютерной технологии и все расширяющейся сферы ее применения.

Особую озабоченность вызывают две тенденции развития преступности в сфере высоких технологий.

Во-первых, благодаря транснациональным информационным сетям, прежде всего Интернету, такая преступность может миновать любые границы.

Во-вторых, она активно используется организованными преступными группировками. Оценка потерь, которые несет экономика в развитых странах Запада, составляет гигантские цифры — порядка миллиардов долларов.

Очевидно, что информационные технологии развиваются с огромной скоростью. Возможности вторжения в частную жизнь или, по крайней мере, по-

тенциальные возможности тоже возрастают. Кроме этих очевидных аспектов (возможности и цена) есть также целый ряд важных факторов, влияющих на нарушения прав человека:

– глобальность, то есть исчезновение географических границ для потока данных (развитие Интернета — вот, возможно, наиболее известный тому пример);

– конвергенция, то есть падение технологических барьеров между системами (современные информационные системы беспрепятственно взаимодействуют и могут передавать друг другу и обрабатывать разные типы данных);

– мультимедиа, то есть современные формы представления данных и изображений; информация, представленная в одном формате, может быть легко конвертирована в другие форматы [42, с. 35-36].

Связанные с использованием высоких технологий преступления, как правило, выходят за рамки обычных и нередко представляют собой неразрешимые для действующего законодательства задачи. Первоначально столкнувшись с преступностью в сфере высоких информационных технологий, правоохранительные органы начали борьбу с ней при помощи традиционных правовых норм о краже, присвоении, мошенничестве, злоупотреблении доверием. Однако такой подход оказался не вполне удачным, поскольку многие преступления не охватываются составами традиционных преступлений.

Несоответствие криминологической реальности и уголовно-правовых норм потребовали корректировки последних. В настоящее время это происходит в двух направлениях:

1) более широкого толкования традиционных норм (Голландия, Франция);

2) разработка специальных норм (США, Швеция, Англия, Дания и абсолютное большинство других стран).

С учетом изменения видов совершения традиционных преступлений в действующее казахстанское уголовное законодательство введены соответствующие статьи, предусматривающие наказания за определенные виды деяний, совершаемые с использованием компьютерной техники и/или в отношении компьютерной информации, а также принят ряд нормативных актов, регламентирующих вопросы электронного документооборота и информатизации [43; 44], пользования сетями телекоммуникаций [45], радиоэлектронных средств и высокочастотных устройств [46].

Анализ статистики о зарегистрированных преступлениях и результатах деятельности органов уголовного преследования МВД РК дает представление о росте выявленных преступлений в сфере высоких технологий. В Казахстане в период с 2001-2003 гг. включительно было зарегистрировано всего 18 деяний, в 2004 г. — 15, в 2005 г. — 26, а в 2006 г. уже 83 преступления (рисунок 1). Возрастающее количество рассматриваемых нами преступлений связано с развитием и распространением новых информационных и телекоммуникационных технологий, а также числом пользователей компьютеров и средств связи. При этом следует учитывать, что 90 % преступлений в сфере высоких технологий являются латентными.

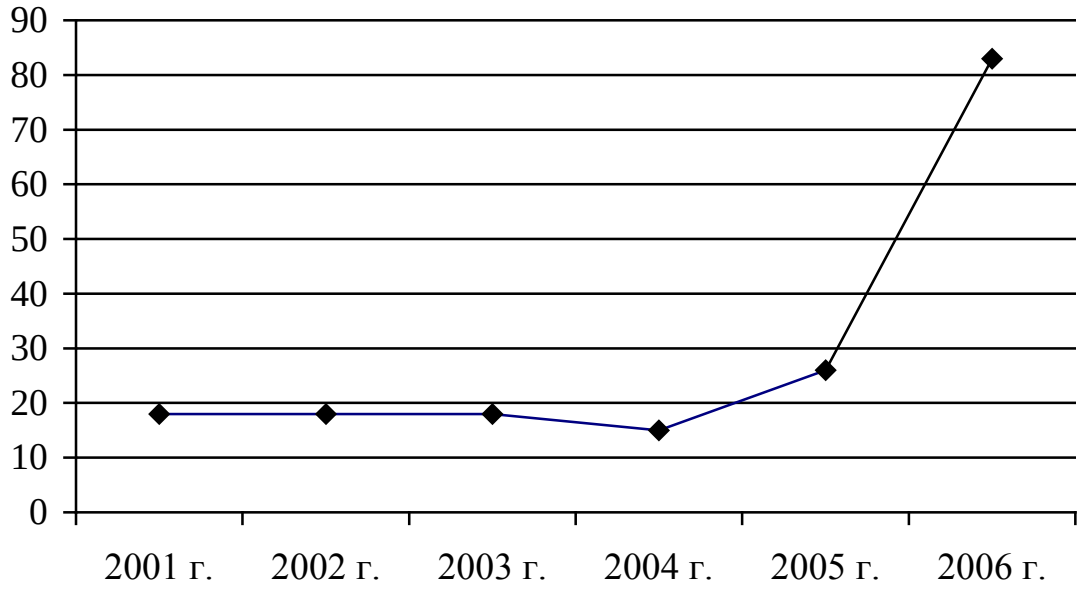

Рисунок 1 — **Динамика преступлений в сфере высоких технологий за период 2001-2006 гг.**

Ввиду стремления преступности (прежде всего организованной) укрепить свои позиции в информационной сфере, возникает объективная необходимость в совершенствовании форм, средств и методов деятельности полиции. Назрел вопрос и о коррективах в кадровой работе, подготовке сотрудников, способных противостоять противоправным явлениям в сфере информационных (высоких) технологий.

Так, в 2003 г. в Республике Казахстан было создано «Управление по организации борьбы с преступлениями в сфере информационных технологий Комитета криминальной полиции МВД РК», деятельность которого направлена на:

– борьбу с преступлениями в сфере компьютерной информации (ЭВМ, их системы и сети, при этом права собственника информации также являются объектом преступного посягательства);

– борьбу с преступлениями в сфере телекоммуникаций (ЭВМ, их системы и сети являются орудием совершения преступлений);

– борьбу с преступлениями, посягающими на конституционные права граждан (неприкосновенность личной жизни, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений);

– борьбу с преступлениями против нравственности (распространение порнографии, Интернет-сводничество, детская порнография);

– борьбу с преступлениями в сфере экономической деятельности (незаконное использование товарного знака, подделка лицензионных продуктов, изготовление или сбыт поддельных платежных карточек и др.);

– непосредственную реализацию международных обязательств в области борьбы с преступлениями в сфере высоких технологий (осуществление опера-

тивного взаимодействия с зарубежными правоохранительными органами по сообщениям о транснациональных компьютерных и телекоммуникационных преступлениях, обмен неотложной информацией, запросами и исполнением розыскных заданий в форматах стран-членов «восьмёрки» и Интерпола).

Кроме того, сотрудники управления:

– участвуют в разработке методик предупреждения, выявления, раскрытия и расследования преступлений в сфере компьютерной информации и телекоммуникаций, а также специальных аппаратных и программных средств для обеспечения оперативно-служебной деятельности;

– подготавливают предложения для внесения изменений в законодательные и ведомственные акты, способствующих устранению пробелов в законодательстве, препятствующих эффективной работе по борьбе с правонарушениями в сфере интеллектуальной собственности и высоких технологий;

– выявляют причины и условия, способствующие правонарушениям в сфере интеллектуальной собственности и высоких технологий, принимают меры к их устранению, полному возмещению ущерба, изъятию денег и ценностей, добытых преступным путем;

– обучают личный состав территориальных подразделений методике и тактике документирования фактов правонарушений в сфере интеллектуальной собственности и высоких технологий.

На сегодняшний день, реализуя возложенные на него задачи, Управление «К», достигло значимых результатов в совершенствовании методов борьбы:

– с правонарушениями на рынке интеллектуальной собственности, своевременного предупреждения и выявления преступлений, связанных с незаконным производством, распространения и использования объектов авторского права и смежных прав. Сотрудниками выявляются лица, занимающиеся подделкой лицензионных продуктов — фильмы на DVD, программное обеспечение, CD-диски. Подразделения «К» активно взаимодействуют со службами безопасности, юристами и техниками предприятий и организаций;

– с преступлениями на сетях телекоммуникаций. В соответствии с «Правилами взаимодействия государственных органов и организаций при внедрении и эксплуатации аппаратно-программных и технических средств проведения оперативно-розыскных мероприятии на сетях телекоммуникаций Республики Казахстан» [47], осуществляют снятие, перехват криминальной информации, используемой в дальнейшем в процессе доказывания по уголовным делам. Полагаем, что данными правилами регламентирована не только возможность осуществления действий по снятию информации, но и определена вероятность проведения системы мероприятий, направленных на обнаружение, фиксацию, исследование и использование в доказывании полученных электронных данных [48, с. 120].

– с преступлениями в банковской сфере. Осуществляется противодействие легализации («отмыванию») денежных средств и другого имущества, добытых преступным путем с помощью высоких технологий. 11 августа 2006 г. проведе-

на рабочая встреча с представителями тринадцати банковских структур Республики Казахстан по вопросам взаимодействия. Результатом встречи явилось подписание «Протокола-намерения по взаимодействию», согласно которому Банки на постоянной основе будут осуществлять обмен информацией о подготавливаемых преступлениях с применением электронных платежных систем; видеозаписи с камер видеонаблюдения, с зафиксированными фактами правонарушений и преступлений, а также лицами, причастными к их совершению инициативно в кратчайшие сроки направлять в подразделения по борьбе с преступлениями в сфере информационных технологий. Кроме того, проработан вопрос о создании эффективной системы обнаружения так называемых «хакерских атак» в режиме реального времени, предусматривающей функцию незамедлительного информирования органов внутренних дел для проведения неотложных оперативно-розыскных мероприятий по пресечению противоправных действий и вопрос о создании «горячей» телефонной линии для взаимообмена информацией, представляющей взаимный интерес; предоставление Банковскими структурами в Комитет криминальной полиции список сотрудников, уволенных за совершение правонарушений, связанных с информационной безопасностью.

Кроме того, при формировании оперативных позиций в среде фирм, представляющих телекоммуникационные услуги (операторов связи) и сетевые услуги (провайдеров) с целью получения оперативной информации о противоправных деяниях и негативных тенденциях внутри этих фирм, а также добывания информации о преступной деятельности третьих лиц, использующих предоставляемые фирмами телекоммуникационные и сетевые ресурсы, сотрудники «К» наладили взаимодействие с компаниями, предоставляющими доступ в Интернет и осуществляющих передачу данных на всей территории Казахстана (323 компании). Имеется соглашение о хранении провайдерами ЛОГ-файлов в течении 3-х месяцев и в случае необходимости предоставление их правоохранительным органам для расследования и раскрытия преступлений. Указанное соглашение является особо значимым, т. к., например, в России и по настоящий день имеется проблема противодействия сотрудникам правоохранительных органов в получении сведений о пользователях Интернет-услуг [49, с. 48-51].

В настоящее время налажено оперативное взаимодействие и проведение совместных розыскных действий с зарубежными правоохранительными органами по пресечению и документированию трансграничных «компьютерных» и «телекоммуникационных» преступлений. Также, в 2006 г. сотрудниками «К» проведена встреча с представителями Франции, Канады по обмену опытом.

Между тем, с учетом особенностей совершения преступлений с использованием высоких информационных технологий на сегодняшний день является актуальным целый комплекс юридических и технических проблем, связанных:

– с неадекватным состоянием национального законодательства (в уголовном законодательстве отсутствует соответствующая общественной опасности содеянного оценка действий, по своей сути являющихся преступлениями, но не нашедших разрешения; в уголовно-процессуальном законодательстве не определены процедуры в отношении материальных объектов, не имеющих веще-

ственных признаков — «электронные» доказательства, «электронные обыски и выемки» и т. п.);

– с несформированностью структур правоохранительных органов, призванных бороться с данными видами преступлений, отсутствие оперативно-розыскных методик по их предупреждению и раскрытию, судебно-следственной практики по такого рода делам, специально обученного личного состава;

– крайне низкой оснащённостью правоохранительных органов специальными аппаратными и программными средствами, без которых эффективная борьба с этим новым видом преступлений практически невозможна;

– низкой профессиональной подготовкой сотрудников спецподразделений.

С учетом масштабов глобальной сети Internet становится все менее вероятным, что все элементы киберпреступности будут ограничены территорией отдельного государства. В процессе проведения расследований правоохранительные органы различных государств должны будут сотрудничать между собой, причем как официально, используя такие рамки и структуры взаимной правовой помощи, как, например, Интерпол, так и неофициально, предоставляя потенциально полезную информацию непосредственно органам другого государства. В связи с правовой помощью при расследовании международной киберпреступности могут возникать дополнительные проблемы. Если в соответствии с внутренним правом одной из сторон не предусмотрены конкретные полномочия на поиск доказательств в электронной среде, такая сторона не в состоянии адекватно реагировать на такие виды преступлений.

В связи с чем становится актуальным определение направленности совершенствования борьбы с «компьютерной» преступностью путем создания Концепции «Стратегия и тактика борьбы с преступностью в сфере высоких информационных технологий», а также внесения дополнений в уголовно-процессуальное законодательство.

Так, диссертант предлагает внести дополнение в ч. 11 ст. 126 УПК РК «Закрепление доказательств» после слов «киносъемка, фотосъемка» словами «программные средства, использующих технологию оперирования информацией» и далее по тексту; а также после слов «с приведением технических характеристик использованных научно-технических средств ...» словами «при применении программных средств, использующих технологию оперирования информацией, в протоколе указываются: наименование продукта, версия, код продукта, операционная система в которой используется программное средство».

Анализируя спорные точки зрения, существующие в юридической литературе, автор отмечает, что существенную помощь в исследовании какого-либо предмета оказывает проведение классификации этого предмета или явления. Аналогично понятию преступлений в сфере высоких информационных технологий в литературе нет единого мнения о том, каким образом и по каким критериям классифицировать преступления в этой сфере. Одной из первых попыток в науке было предложенное Ю. М. Батуриным разделение преступлений по способу их совершения:

– методы перехвата;

– методы несанкционированного доступа;

– методы манипуляции [50, с. 31].

В каждой из указанных групп Ю. М. Батурин выделяет группы способов, название и описание которых будет дано нами в следующих разделах диссертации.

Определенный интерес представляет предложенная В. А. Мещеряковым классификация, исходящая из идеи не столько преступлений, сколько совокупности возможных противоправных посягательств в этой сфере [51, с. 16].

1. Неправомерное завладение информацией или нарушение исключительного права ее использования:

– неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения);

– неправомерное завладение информацией как товаром;

– неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

2. Неправомерная модификация информации:

– как товара с целью воспользоваться ее полезными свойствами (снятие защиты);

– как идеи, алгоритма и выдача за свою (подправка алгоритма);

– как совокупности фактов, сведений.

3. Разрушение информации:

– разрушение информации как товара;

– уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами:

– распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу и личности;

– разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ;

– преступная халатность при разработке (эксплуатации) программного обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям:

– неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.);

– информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов).

Указанная классификация имеет ощутимое преимущество перед остальными — ее основанием являются не абстрактные юридические модели, а реальные правонарушения, совершаемые в настоящее время.

Значительный опыт уголовно-правовой классификации преступлений в сфере высоких информационных технологий накоплен в ведущих промышленно развитых государствах мира. Одной из наиболее распространенных из существующих классификаций является кодификатор рабочей группы Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов [52, с. 13]. В данном кодификаторе, утвержденном Генеральным Секретариатом Интерпола, преступлениям в сфере высоких информационных технологий присвоен индекс «Q» — компьютерные, в связи с применением компьютерной техники как средства преступной деятельности. В соответствии с названным кодификатором, все компьютерные преступления классифицированы следующим образом:

1. *QA — несанкционированный доступ и перехват*:

– QAH — компьютерный абордаж (несанкционированный доступ);

– QAI — перехват информации с помощью специальных технических средств;

– QAT — кража времени (уклонение от платы за пользование автоматизированных информационных систем);

– QAZ — прочие виды несанкционированного доступа и перехвата.

2. *QD — изменение компьютерных данных*:

– QDL — логическая бомба (набор команд, срабатывающих при определенном условии);

– QDT — троянский конь (набор команд, встраиваемых в иную программу с сохранением ее работоспособности);

– QDV — компьютерный вирус (деструктивная программа, способная к автономному распространению — определение и подробное описание находится ниже);

– QDW — компьютерный червь (программа, способная к автономному распространению через компьютерную сеть);

– QDZ — прочие виды изменения данных.

3. *QF — компьютерное мошенничество*:

– QFC — мошенничество с банкоматами;

– QFF — компьютерная подделка (карточки и иные устройства);

– QFG — мошенничество с игровыми автоматами;

– QFM — манипуляции с программами ввода-вывода (ввод неверных данных и анализ результатов этих программ);

– QFP — мошенничества с платежными средствами (как правило, хищения денежных средств — наиболее распространенный вид компьютерных преступлений);

– QFT — телефонное мошенничество (посягательства на системы телекоммуникационных услуг);

– QFZ — прочие компьютерные мошенничества.

4. *QR — незаконное копирование*:

– QRG — компьютерных игр;

– QRS — прочего программного обеспечения;
– QRT — топологии полупроводниковых устройств;
– QRZ — прочее незаконное копирование.
5. *QS — компьютерный саботаж*:
– QSH — в отношении аппаратного обеспечения (нарушение работы ЭВМ);
– QSS — в отношении программного обеспечения (уничтожение, блокирование информации);
– QSZ — прочие виды саботажа.
6. *QZ — прочие компьютерные преступления*:
– QZB — с использованием компьютерных досок объявлений;
– QZE — хищение информации, составляющей коммерческую тайну;
– QZS — передача информации конфиденциального характера;
– QZZ — прочие компьютерные преступления.

Данная классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола. К достоинствам данной классификации следует отнести ее универсальность, распространенность (используется в более чем 100 странах), а также возможность ее дополнения с помощью индекса «Z» — отражающей прочие виды преступлений и позволяющей совершенствовать и дополнять используемую классификацию.

Однако приведенные выше системы классификации, как и ряд других, например, «минимальный» и «необязательный» списки нарушений «Руководства Интерпола по компьютерной преступности», страдают одним общим недостатком — в них происходит смешение уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что приводит к неоднозначности толкования и еще большей неопределенности понятия «преступлений в сфере высоких информационных технологий» и соответственно затрудняет определение категорий преступлений.

Наиболее удачной на тот период времени, по нашему мнению, является классификация, предложенная Марком Экенвайлером, в которой он выделяет три основные категории (с дальнейшей дифференциацией) в зависимости от способа использования компьютера при совершении преступлений [53]:

1. Компьютер является объектом правонарушения, когда цель преступника — похитить информацию или нанести вред интересующей его системе:

– изъятие средств компьютерной техники с находящейся в ней информацией;

– хищение информации;

– хищение услуг (получение несанкционированного доступа к какой-то системе с целью безвозмездного пользования предоставляемыми ею услугами);

– повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы — объекта несанкционированного доступа.

2. Компьютеры используются как средства, способствующие совершению преступления:

– как средство совершения традиционных преступлений (как правило, мошенничество);

– как средство атаки на другой компьютер, средство совершения иного компьютерного преступления.

3. Компьютер используется как запоминающее устройство (например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек и т. п.)

Полагаем, что третья категория данной классификации представляется нам излишней, поскольку использование компьютеров в качестве запоминающих устройств полностью входит во вторую категорию — в качестве средств совершения преступлений.

В целом, поддерживая точку зрения М. Экенвайлера, относительно направления классификации, с учетом современного состояния преступной деятельности при совершении исследуемой преступной категории, сформированной понятийным аппаратом [25, с. 32], полагаем, что классификацию преступлений в сфере высоких информационных технологий следует осуществлять по следующим критериям:

– высокоточное оборудование, устройства и программные средства, использующие технологию оперирования информацией, компьютерная информация — являются объектом правонарушения (в данную категорию входят противоправные действия, направленные на проведение незаконных операций над компьютерной информацией, несанкционированный доступ в компьютерные системы, нарушение деятельности их работы, незаконное изъятие, уничтожение, выведение из строя компьютерной техники и т. п.);

– высокоточное оборудование, устройства и программные средства, использующие технологию оперирования информацией, компьютерная информация — используются как орудия и средства, способствующие совершению преступления (к данной категории относятся правонарушения, реализованные с применением различных способов их совершения — распространение вируса, мошенничество, подделка платежных карточек, перехват сообщений и т. п.).

Предложенная классификация позволит систематизировать уголовно-правовые аспекты определения видов преступлений в сфере высоких информационных технологий, а также определить способы совершения, конкретные приемы их применения, используемые при этом технические средства, методы подготовки и исполнения преступления и множество иных обстоятельств, имеющих следственно-оперативное значение при расследовании и раскрытии преступлений в сфере высоких информационных технологий.

2 КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Преступления в сфере высоких информационных технологий многоаспектны и потому могут относиться к самым различным видам преступных посягательств и отличаться не только по объекту посягательства, но и по способам, мотивам и другим признакам. Поэтому криминалистическая характеристика преступлений в сфере высоких информационных технологий отличается определенной спецификой. Изучение материалов уголовных дел, опрос сотрудников органов внутренних дел и других правоохранительных органов, занимающихся расследованием преступлений в сфере компьютерной информации (Приложения А, Б), личный опыт и наблюдения позволяют сделать вывод, что практические работники правоохранительных органов испытывают потребность в научно обоснованной методике расследования данной категории преступлений. В целях научного осмысления проблемы, прежде всего, необходимо разработать криминалистическую характеристику данной группы преступлений. Это, по мнению Н. П. Яблокова, — обязательный этап разработки методик по расследованию отдельных видов преступлений [54, с. 32-33].

В основе научного исследования любого явления лежит изучение гносеологической сущности явления, определение составных элементов явления и подробная характеристика данных элементов. Несомненно и то, что сущность любого научного исследования предопределяется условиями, направлениями, границами изучаемого материала, лежащего в основе исследования. В данном случае, криминалистическая характеристика не только выполняет важнейшую функцию дефиниционного определения основ исследования, но и определяет его дальнейшее развитие, является той частью работы, которая во многом предопределяет. С точки зрения узкокриминалистического понимания необходимость ее существования зиждется на том, что всякое преступление представляет собой событие, характеризующееся совокупностью присущих только лишь ему индивидуальных признаков и особенностей, выделение и описание которых, на основе эмпирического обобщения опыта расследования конкретного вида преступлений, может являться основой для создания методик расследования преступлений [55]. В этой связи, криминалистическая характеристика преступлений в сфере высоких информационных технологий имеет большое значение в исследовании данного преступного явления, является его основой.

Вместе с тем, многообразие точек зрения на сущность криминалистической характеристики заставляет нас уделить внимание самому понятию «криминалистическая характеристика», как обстоятельству, определяющему его содержание. Так, изучением данной дефиниции занималась плеяда таких ученых как: Е. Г. Джакишев [56],Г. А. Мозговых [57; 58], А. А. Эйсман [59], И. Ф. Герасимов [60], И. В. Крылов [61], В. Г. Танасевич, В. В. Образцов [62], А. Н. Васильев [63], И. М. Лузгин [64], Н. А. Селиванов [65], А. Н. Колесниченко [66] и

др. Проведенный анализ работ указанных авторов позволил сделать общий вывод о том, что криминалистическая характеристика:

– динамическая система (совокупность) соответствующих взаимосвязанных общих и индивидуальных признаков преступления, ярче всего проявляющихся в способе, механизме преступного деяния, обстановке его совершения и в отдельных чертах личности его субъекта, данные которой имеют важное значение для разработки методов расследования [67, с. 15];

– представляет собой совокупность таких данных о нем, которые способствуют раскрытию преступлений, имеют криминалистическое значение [68, с. 454];

– система описания криминалистически значимых признаков вида, группы и отдельного преступления, проявляющихся в особенностях способа, механизма и обстановки их совершения, дающую представление о преступлении, личности его субъекта и иных обстоятельствах, об определенной преступной деятельности и имеющую своим назначением обеспечение успешного решения задач раскрытия, расследования и предупреждения преступления [69, с. 324];

– абстрактное научное понятие, — результат научного анализа определенного вида преступной деятельности (вида или рода преступления), обобщение его типичных признаков и особенностей [70, с. 63].

Безусловно, каждый из авторов перечисленных определений криминалистической характеристики привел достаточно доводов в защиту верности собственного понятия криминалистической характеристики, однако, полагаем, что не имеет смысла приводить все эти доводы. Однако хотелось бы отметить, что, например, Н. Г. Шурухнов определяет криминалистическую характеристику преступления как отражение системы криминалистических черт, свойств, признаков преступления, отобразившихся в объективной действительности. «Она содержит данные о типичных способах совершения и сокрытия преступления, механизме преступного посягательства, следах, обстановке, в которой готовилось и происходило преступное событие, предметах преступного посягательства, чертах личности преступника и потерпевшего, а также обстоятельствах, способствующих совершению преступлений» [71, с. 25]. Роль этих данных состоит в том, что они позволяют увидеть связь между различными обстоятельствами совершения преступления и в условиях недостатка исходной информации выдвинуть обоснованные версии, выбрать оптимальный путь по установлению лиц, совершивших преступление [72, с. 21]. Думается, безусловно, прав В. П. Лавров, отмечавший, что знание криминалистической характеристики позволяет делать выводы об оптимальных путях раскрытия и расследования преступления [73, с. 85].

Между тем, следует отметить, что криминалистическая характеристика преступлений в сфере высоких информационных технологий только начинает формироваться, и поэтому вполне объяснимы те трудности, которые возникают в этом процессе. Имеющейся эмпирической базы, основанной на собранных материалах из практики деятельности правоохранительных органов, явно недостаточно. Однако, необходимость разработки криминалистической характери-

стики и методики расследования преступлений в сфере высоких информационных технологий продиктована реализацией на практике одного из фундаментальных принципов деятельности правоохранительных органов в борьбе с преступностью — наступательности. В связи с чем полагаем, что с учетом существенного своеобразия основных структурных элементов преступлений в сфере высоких информационных технологий возникает необходимость определения собственного содержания криминалистической характеристики указанного вида преступлений. Изложенная позиция подтверждается Р. С. Белкиным о том, что на сегодняшний день понятие «криминалистическая характеристика» является абстрактным и развивающимся, что в конечном итоге признают все указанные авторы [74, с. 318].

Исходя из данных обстоятельств, следует отметить, что криминалистическая характеристика преступлений в сфере высоких информационных технологий содержит систему обобщенных данных [75, с. 55] о типичных способах совершения преступления, орудиях и средствах, применяемых при совершении преступлений в сфере высоких технологий; обстановке, месте и времени совершения преступлений; о личности преступника, мотивах и целях его преступного поведения. Именно такой структуры криминалистической характеристики мы и придерживаемся в представленном исследовании.

Так, рассмотрение вопроса о криминалистической характеристике преступлений в сфере высоких информационных технологий не было бы полным без выделения такого элемента как способ совершения. Этот элемент является основой характеристики преступлений. Под способом совершения преступления понимается система объединенных единым замыслом действий преступника (и связанных с ними лиц) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных с использованием соответствующих орудий и средств [73, с. 75-84; 74, с. 183-192; 76, с. 26; 77, с. 105-107]. В целом, поддерживая смысл данного определения и определяя содержание способа совершения преступления, В. Б. Вехов включает в данное понятие и наличие следов, оставляемых преступником, что позволяет определить методику расследования совершаемых преступлений и дает следующее определение, где под способом совершения преступления в криминалистическом смысле обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и собственно определить наиболее оптимальные методы решения задач раскрытия преступления [78, с. 18].

Иными словами, способ совершения преступления слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступления, представляющих в информационном плане своеобразную модель преступления. Способ совершения преступления всегда является

результатом совокупного действия значительного числа факторов. И чем больше будут они проявляться в действиях, тем больше следов будет оставлять преступник, тем большей информацией будет располагать следователь для выдвижения следственных и розыскных версий. При этом под следами преступления понимаются любые изменения среды, возникшие в результате совершения в этой среде преступления [74, с. 57].

Следы совершения преступления в сфере компьютерной информации в силу специфики рассматриваемого вида преступлений редко остаются в виде изменений внешней среды. Они в основном не рассматриваются современной трасологией, поскольку в большинстве случаев носят информационный характер, т. е. представляют собой те или иные изменения в компьютерной информации, имеющие форму ее уничтожения, модификации, копирования, блокирования. Как справедливо отмечает А. В. Касаткин: «при современном развитии вычислительной техники и информационных технологий “компьютерные следы” преступной деятельности имеют широкое распространение. Это должно учитываться следователями и оперативными работниками в их деятельности по собиранию доказательств наряду с поиском уже ставших традиционными следов» [79, с. 14].

На основании изложенного представляется целесообразным следы преступлений в сфере высоких технологий разделить на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, а также следы-вещества и следы-предметы) и нетрадиционные — информационные следы.

К первому типу относятся материальные следы. Ими могут являться какие-либо рукописные записи, распечатки и т. п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере и т. д.), а также на магнитных носителях и CD-ROM дисках.

Информационные следы образуются в результате воздействия (уничтожения, модификации, копирования, блокирования) на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Прежде всего, они остаются на машинных носителях информации и отражают изменения в хранящейся в них информации (по сравнению с исходным состоянием).

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств в качестве инструмента для проникновения в информационные системы или воздействия на них. Характерной особенностью данного вида преступной деятельности является то обстоятельство, что место совершения непосредственно преступных действий и место, где наблюдаются и материализуются их результаты, могут находиться на значительном удалении друг от друга (например, в разных точках земного шара). В этих случаях при неправомерном доступе и распространении вредоносных программ, а также при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети, следовая картина включает в себя:

а) следы на машинных носителях, посредством которых действовал преступник на своем рабочем месте (рисунок 2) и возле машинных носителей, принадлежащих преступнику (рисунок 3);

б) следы на «транзитных» (коммуникационных) машинных носителях, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися нападению (рисунок 4);

в) следы на машинных носителях информационной системы, в которую осуществлен неправомерный доступ (рисунок 5).

С целью наглядного восприятия следовой картины рассматриваемых видов преступлений, в качестве примера, приведем разработанные отдельными учеными схемы отображения следов [80, с. 57-58].

Изменения в оперативном запоминающем устройстве (ОЗУ) ЭВМ возможно зафиксировать лишь в ходе следственного осмотра технических устройств в случаях, когда они на момент осмотра включены, т. е. фактически преступник пойман на месте и осмотр устройств является действием, сопутствующим задержанию. В иных случаях информация в ОЗУ достаточно быстро изменяется в ходе исполнения программ и о результатах ее изменения можно судить лишь по показаниям очевидцев. Специальным случаем фиксации изменений в ОЗУ являются оперативные или следственные мероприятия, обеспечивающие наблюдение за криминальными действиями и вывод данных из ОЗУ на какой-либо долговременный носитель информации.

Следы изменений в файловой системе могут наблюдаться как в ходе изменений непосредственно пользователем или администратором системы, а в случае следственно-оперативных мероприятий и следственными работниками, с помощью соответствующих программных средств. Результаты изменений могут быть зафиксированы на долговременный носитель специальными программно-техническими средствами контроля доступа, а также установлены в результате сравнения копий, сохраненных резервным копированием файлов и их структуры. Явными следами криминальных действий являются обнаруженные на конкретном машинном носителе копии скопированных «чужих» файлов, специализированное программное обеспечение, предназначенное для «взлома» систем и файлов, и др. Сходные следы могут быть обнаружены и на машинных носителях, в которые проник преступник.

С уголовно-правовой позиции способ совершения преступления представлен в общем виде, например, способ открытого или тайного похищения, проникновение в помещение и т. д., в данном случае безразличны приемы тайного похищения, конкретные способы проникновения в помещение и т. д.

С криминалистической же точки зрения способ совершения преступления всегда конкретен и у него имеется немало таких граней, которые имеют важное следственно-оперативное значение (например, распространенность данного способа, конкретные приемы его применения, используемые при этом технические и иные средства, их конструктивные особенности, методы использования при подготовке и исполнении преступления, а также сведения о том, как подготавливается преступление, каким образом проводятся тренировки, как и где из-

готавливаются или приспосабливаются необходимые орудия и другие технические средства, каковы источники их получения, и т. п.).

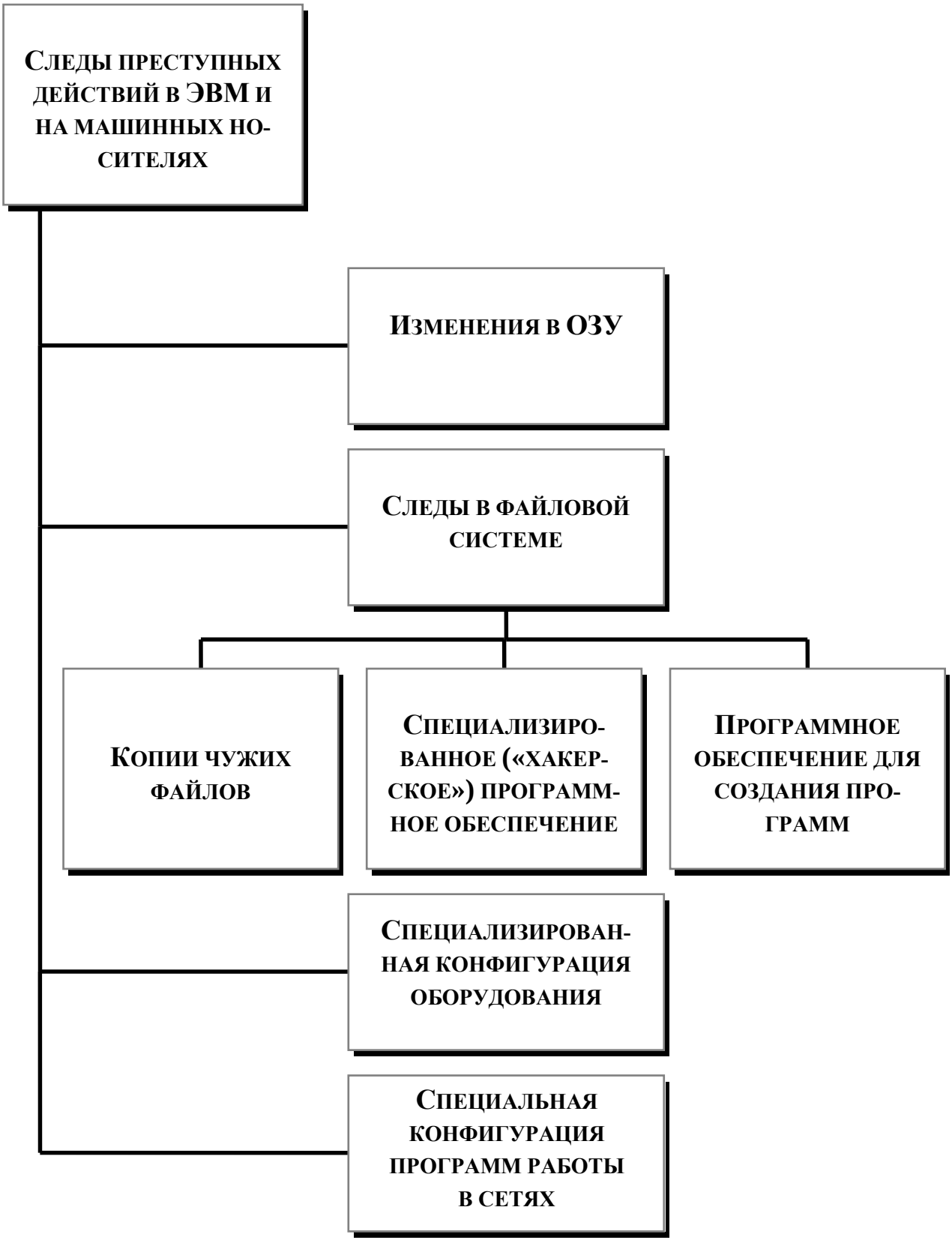

Рисунок 2 — **Виды следов преступной деятельности в ЭВМ и на машинных носителях, принадлежащих преступнику**

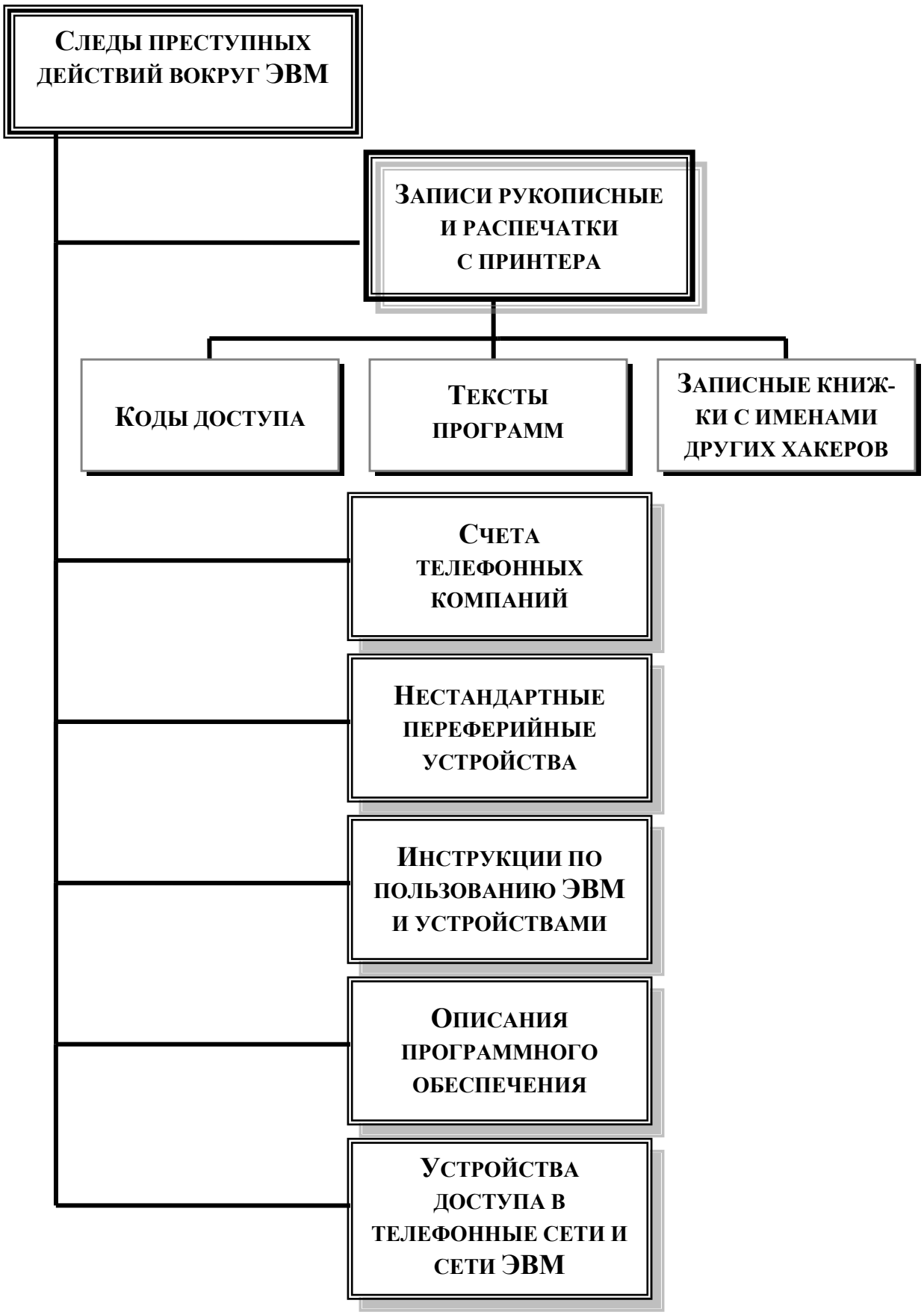

Рисунок 3 — **Виды следов преступной деятельности возле ЭВМ и на машинных носителях, принадлежащих преступнику**

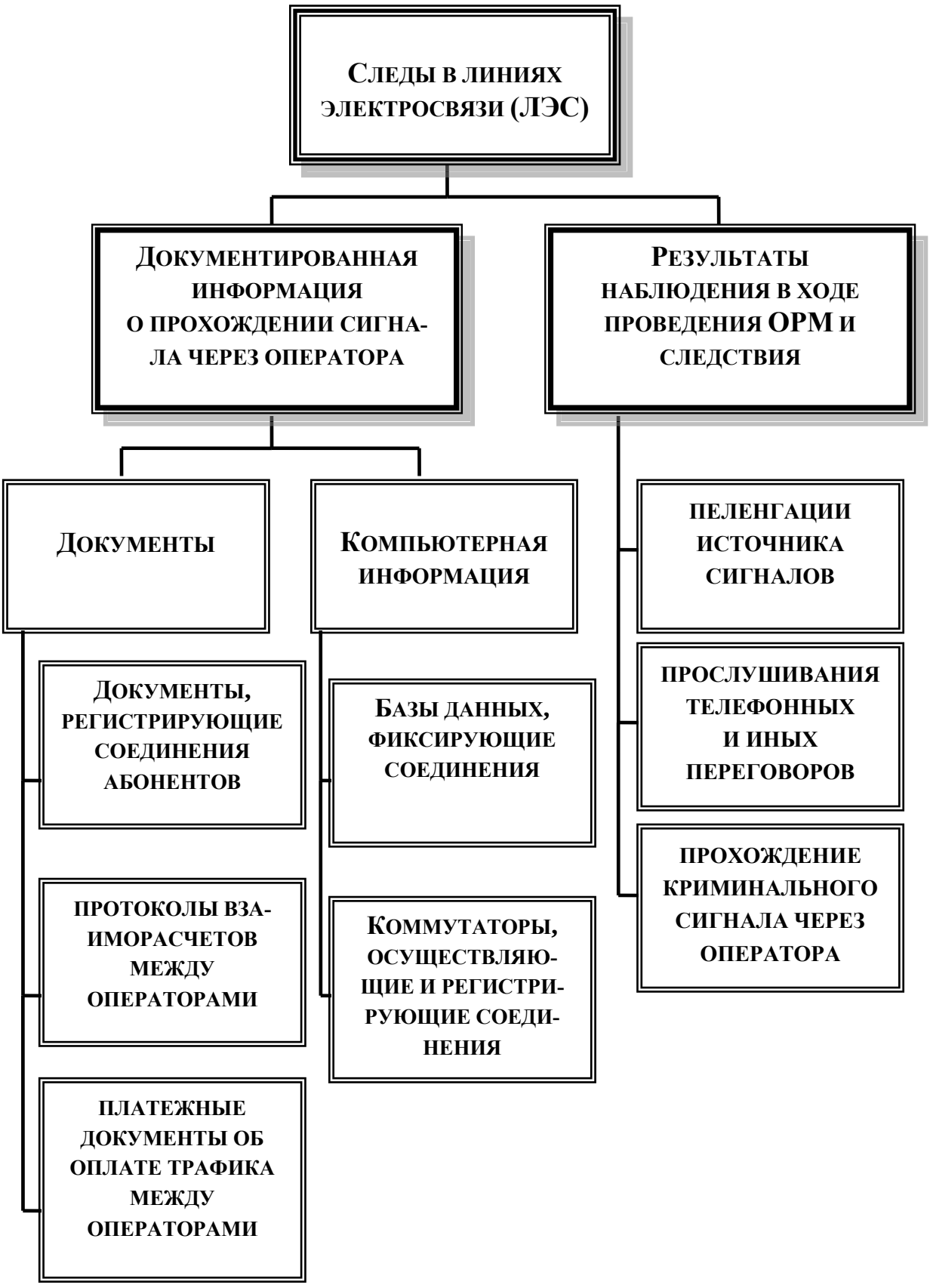

Рисунок 4 — **Виды следов преступной деятельности на «транзитных» машинных носителях**

Рисунок 5 — **Виды следов преступной деятельности на машинных носителях, принадлежащих потерпевшему**

В настоящее время в отечественной и зарубежной криминалистической науке не существует сколько-нибудь определенных понятий в вопросах характеристики способов совершения преступлений в сфере высоких информационных технологий, их конкретных названий и классификации.

Эта проблема настолько нова для науки, что находится пока лишь в стадии осмысления и теоретических разработок. Особенно это касается отечественной криминалистической науки, которая всерьез стала заниматься этими вопросами лишь с начала 90-х годов прошлого столетия, тогда как зарубежные исследователи — только с конца 70-х годов. В этом плане мы отстаем от зарубежных исследователей почти на 20 лет [81, с. 3].

У наших зарубежных коллег в этом плане уже имеется ряд ценных, с научной и практической точек зрения, разработок, которые необходимо использовать при изучении и решении аналогичных вопросов в отечественной криминалистической науке с учетом определенных объективных и субъективных поправок и приближений, диктуемых реальностью функционирования и развития

нашего общества, его политическими, правовыми, социальными и экономическими составляющими.

В настоящее время в юридической литературе существуют различные точки зрения в вопросах выделения, классификации и названия способов совершения преступлений.

Например, Американский Национальный институт компьютерной безопасности и ФБР провели опрос о наиболее распространенных компьютерных преступлениях. В опросе было учтено мнение только тех 269 компаний, которые сумели измерить свои потери:

– финансовое мошенничество (средний ущерб 957387 $ в год);
– кража конфиденциальной информации (954666 $);
– мошенничество, касающееся средств связи (647437 $);
– несанкционированный доступ (181436 $);
– диверсия (164840 $);
– проникновение в систему (132250 $).

Основными способами несанкционированного получения информации, сформулированными по данным зарубежной печати, являются:

– применение подслушивающих устройств (закладок);
– дистанционное фотографирование;
– перехват электронных излучений;
– мистификация (маскировка под запросы системы);
– перехват акустических излучений и восстановление текста принтера;
– хищение носителей информации и производственных отходов (сбор мусора);
– считывание данных из массивов других пользователей;
– копирование носителей информации с преодолением мер защиты;
– маскировка под зарегистрированного пользователя;
– использование программных ловушек;
– незаконное подключение к аппаратуре и линиям связи;
– вывод из строя механизмов защиты; и др. [82].

В связи с отсутствием аналогичных отечественных статистических данных по рассматриваемому кругу вопросов можно с определенной степенью условности оперировать данными зарубежных исследований применительно к отечественной практике. Тем более что материалы конкретных уголовных дел подтверждают правоту зарубежных исследователей.

На основе анализа конкретных уголовных дел по преступлениям, совершенным с использованием средств компьютерной техники, а также изучения специальной литературы можно выделить свыше 20 основных способов совершения преступлений и около 40 их разновидностей, число которых постоянно увеличивается по причине использования преступниками различных их комбинаций и логической модификации алгоритмов [83, с. 15].

Как нами было уже отмечено, на сегодняшний день, несмотря на неоднократное исследование различными учеными [78, с. 49-105; 84, с. 18-34; 85,

с. 83-101; 86, с. 65-70], в криминалистике нет единой классификации способов совершения преступлений в сфере высоких информационных технологий.

Так, согласно классификации, предложенной А. Н. Родионовым и А. В. Кузнецовым, способы совершения можно подразделить на:

1) изъятие средств компьютерной техники;

2) неправомерный доступ к компьютерной информации: преступления, совершенные в отношении компьютерной информации, находящейся в глобальных компьютерных сетях; преступления, совершенные в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (сотовый телефон, кассовый аппарат и т. п.);

3) изготовление или распространение вредоносных программ (вирусы, программы-взломщики и т. п.);

4) перехват информации: электромагнитный; непосредственный;

5) нарушение авторских прав (компьютерное пиратство);

6) комплексные методы [86, с. 67].

Ю. М. Батурин, определяя в качестве основного классифицирующего признака метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями, выделяет пять основных групп [50, с. 31]:

1) изъятие средств компьютерной техники (СКТ);

2) перехват информации;

3) несанкционированный доступ к СКТ;

4) манипуляцию данными и управляющими командами;

5) комплексные методы.

При этом к первой относятся традиционные способы совершения преступлений, в которых действия преступника направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимается любое средство вычислительной техники (СВТ). С уголовно-правовой точки зрения подобные преступные деяния будут квалифицироваться по совокупности с соответствующими статьями Уголовного кодекса. Такой способ совершения преступления достаточно прост и традиционен и относится к рассматриваемой группе, как и те, которые связаны с противоправным изъятием различных физических носителей ценной информации — дискет, оптических и магнитооптических компакт-дисков, пластиковых карт, интегральных микросхем и т. п.

Ко второй группе способов Ю. М. Батурин относит те, которые основаны на получении преступником компьютерной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемые в оперативно-розыскной деятельности. К ним, в частности, относятся:

1) пассивный (бесконтактный) перехват, осуществляемый путем дистанционного перехвата электромагнитных излучений, испускаемых при работе СВТ;

2) активный (контактный) перехват, осуществляемый путем непосредственного подключения к СВТ или системе передачи данных с помощью различных штатных оперативно-технических и специально изготовленных, разработан-

ных, приспособленных и запрограммированных средств негласного получения информации, иногда с использованием скрытых (замаскированных, зашифрованных) каналов. В данном случае преступник может целенаправленно воздействовать на СВТ в целом, его составляющие, на систему санкционирования доступа, на каналы передачи данных и на саму компьютерную информацию.

К третьей группе относятся способы совершения преступления, направленные на получение преступником несанкционированного доступа к СВТ, например, с использованием метода легендирования («электрик», «мастер по ремонту телефонов», «сотрудник сервисной обслуживающей организации» и т. п.), а также путем несанкционированного подключения к системе передачи компьютерной информации с целью перехвата управления вызовом абонента сети «на себя» и т. п.

Четвертая группа — это действия преступника, связанные с использованием методов манипуляции входными-выходными данными и управляющими командами средств вычислительной техники. В качестве наглядных примеров можно привести такие способы, как «троянский конь», «троянская матрешка», «салями», «воздушный змей», «временная» или «логическая бомба», «люк», «компьютерный вирус» и т. п.

К пятой группе относятся комплексные способы совершения преступления, основанные на применении преступником двух и более способов различных групп, причем один из них всегда используется как основной, а другие выполняют вспомогательные функции, например, сокрытие следов преступления.

Как справедливо отмечает Ю. В. Гаврилин, данная классификация не лишена недостатков. Во-первых, фактически авторами за основу классификации взят непосредственный объект преступного посягательства, а не способ совершения преступления. Во-вторых, неправомерный доступ к компьютерной информации, как показано нами выше, совершается гораздо большим количеством способов, чем отметили авторы (в частности, ими не отмечены непосредственные способы). В-третьих, способы перехвата информации относятся к способам неправомерного доступа к ней, и выделение их в качестве самостоятельной группы необоснованно. И, в-четвертых, изъятие средств компьютерной техники представляет собой преступление против собственности, а не в сфере компьютерной информации [87, с. 55-56].

В связи с изложенными доводами, полагая, что представляется более целесообразным рассмотреть отдельно способы совершения неправомерного доступа к компьютерной информации; создания, использования и распространения вредоносных программ для ЭВМ и нарушения правил эксплуатации ЭВМ, их системы или сети, Ю. В. Гаврилин предлагает свою классификацию способов и объединяет их в три основные группы [87, с. 19-20].

Первая группа — это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а также может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд с компьютера, на котором информация находится. Непосредственный доступ может осуществляться как лицами, работающими с

информацией (имеющими отношение к этой работе), так и лицами, специально проникающими в закрытые зоны и помещения, где производится обработка информации. Например, человек, имеющий умысел на противоправный доступ к компьютерной информации, держа в руках определенные предметы, указывающие на его «принадлежность» к работе на компьютере (дискеты, распечатки и пр.), прохаживается около запертой двери помещения, где расположен терминал. Дождавшись, когда в названное помещение войдет работающий в нем сотрудник, он входит туда вслед за ним, а потом через определенный промежуток времени при благоприятной для этого обстановке совершает неправомерный доступ к компьютерной информации.

Вторая группа способов совершения рассматриваемого преступления включает способы опосредованного (удаленного) доступа к компьютерной информации. При этом неправомерный доступ к определенному компьютеру и находящейся на нем информации осуществляется с другого компьютера, находящегося на определенном расстоянии, через компьютерные сети. Способы опосредованного доступа к компьютерной информации, в свою очередь, можно разделить на две подгруппы: способы преодоления парольной, а также иной программной или технической защиты и последующего подключения к чужой системе; способы перехвата информации.

К способам первой подгруппы относятся:

1. Подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе.

2. Проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не «отзовется чужой» компьютер).

3. Проникновение в компьютерную систему с использованием чужих паролей, выдавая себя за законного пользователя. Подбор паролей может осуществляться двумя методами:

1) путем простого перебора всех возможных сочетаний символов до тех пор, пока не будет установлена нужная комбинация:

а) разновидностью способа получения пароля для последующего незаконного вхождения в компьютерную систему является так называемый социальный инжиниринг («обратный социальный инжиниринг»);

б) способы непосредственного, электромагнитного и других видов перехвата;

2) «интеллектуальный» подбор паролей на основе имеющихся «словарей» наиболее распространенных паролей, систематизированных по определенным тематическим группам.

Третью группу способов совершения анализируемого преступления составляют смешанные способы, которые могут осуществляться как путем непосредственного, так и опосредованного (удаленного) доступа, а также создание, использование и распространение вредоносных программ для ЭВМ.

Анализируя классификацию способов, предложенных Ю. В. Гаврилиным, полагаем, что она также не лишена недостатков. Выделенные группы страдают загруженностью различных подгрупп, которые в свою очередь содержат свои подгруппы. Кроме того, отнесение перехвата к группе опосредованного доступа к компьютерной информации довольно спорно, так как перехват может осуществляться как непосредственно, с помощью подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, так и опосредованно — без прямого подключения.

На основе исследования классификаций способов совершения преступлений, в целях устранения выявленных недостатков, определения наиболее практичной, с позиции изучения, определения методов расследования, тактики производства следственно-оперативных действий, нами предлагается собственная классификация способов совершения преступлений с подробным описанием наиболее распространенных способов, применяемых компьютерными преступниками.

Так, способы совершения преступлений в сфере высоких технологий можно объединить в три основные группы:

1) несанкционированный доступ к СКТ;

2) манипуляция данными и управляющими командами;

3) комплексные методы.

К **первой группе** способов относятся действия преступника, направленные на изъятие средств компьютерной техники, информации (например, незаконное изъятие физических носителей, на которых находится ценная информация), на получение несанкционированного доступа к средствам компьютерной техники, к компьютерным системам, компьютерной информации, с применением легендирования («Маскарад»)» или путем нахождения слабых мест в ее защите, при использовании ошибки или неудачи в логике построения программы путем анализа ее работы («За хвост», «Компьютерный абордаж», «Поиск бреши» и т. п.).

Ко **второй группе** способов относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники в целях осуществления подмены входных и выходных данных в процессе автоматизированной обработки документов или внесение умышленного изменения в существующую программу, заведомо приводящего к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т. д. («троянский конь», «салями», «логическая бомба», «асинхронная атака», «компьютерный вирус).

К **третьей группе** способов относятся комплексные методы, под которыми понимается использование преступником двух и более способов, а также их различных комбинаций при совершении преступления (отличительным свойством обладает такой способ совершения компьютерного преступления как перехват, сочетающий в себе физическую и электронную формы действий).

Рассмотрим их более подробно.

Первая группа. Рассматривая способы совершения преступлений, в которых преступник изымает чужое имущество — средства компьютерной техники с целью завладения находящей в ней информации, — то следует отметить, что с уголовно-правовой точки зрения подобные преступления будут квалифицироваться соответствующими статьями уголовного законодательства, например, шпионаж, хищение, разбой, вымогательство и т. п. Однако, характерной отличительной чертой данной группы способов будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления будут использоваться иные инструменты, технические устройства и приспособления (или без их использования), не являющиеся средствами компьютерной техники. Сюда также можно отнести и различные способы совершения преступлений, связанных с противоправным изъятием различных физических носителей информации: магнитных лент и дисков, оптических и магнитооптических дисков, электронных кредитных карточек, электронных акций, услуг и т. п. Например, из производственной лаборатории преступниками был похищен магнитный диск (дискета), на котором находилась медицинская программа по иммунологии, оцениваемая специалистами в 720 тыс. долларов США [88]. Еще одним примером совершения неправомерного доступа к компьютерной информации может являться дело по обвинению К. по ч. 1 ст. 227 УК РК [89]. В ходе расследования было установлено, что он, находясь на работе в качестве электромеханика районного узла электрической связи, на принесенную с собой дискету скопировал с компьютера готовящийся к изданию телефонный справочник г. Павлодара. Эту дискету он принес домой и скопировал полученную информацию на жесткий диск своего компьютера, а затем на принтере отпечатал 4 экземпляра названного справочника. Таким образом, К. умышленно, незаконно скопировал информацию, хранившуюся в электронно-вычислительной машине.

Полагаем, что именно наличие средств компьютерной техники, информации как объекта совершаемых преступлений, является основанием отнесения данных способов совершения преступлений к преступлениям в сфере высоких информационных технологий. Несомненно, данные способы совершения преступлений достаточно полно изучены отечественной криминалистической наукой, поэтому нет надобности рассматривать их подробнее.

Необходимо также отметить, что описанные способы в настоящее время менее распространены по причине децентрализации обработки информации. Практика показывает, что преступники компьютерную информацию чаще перехватывают при ее передаче по телекоммуникационным каналам и компьютерным сетям. Сделать это им и проще, и безопаснее, чем при непосредственном проникновении в помещение. Эти методы имеют свои специфические названия, достаточно распространенные как за рубежом, так и в отечественной практике.

1. ***«Следование за дураком» (pigbacking).*** Типичный прием физического проникновения хорошо известен специалистам, занимающимся вопросами со-

вершенствования оперативно-розыскной деятельности. Он заключается в следующем: держа в руках предметы, связанные с работой на компьютерной технике (элементы маскировки), нужно ожидать кого-либо, имеющего санкционированный доступ, возле запертой двери, за которой находится предмет посягательства. Когда появляется законный пользователь, остается только войти внутрь вместе с ним или попросить его помочь донести якобы необходимые для работы на компьютере предметы. Еще одной разновидностью этого способа является ситуация, когда преступник получает несанкционированный доступ к средствам компьютерной техники путем прямого подключения к ним. Подключиться можно с помощью телефонной проводки. Преступление совершается в тот момент, когда сотрудник, который отвечает за работу средства компьютерной техники, ненадолго покидает свое рабочее место, оставляя технику в активном режиме. Этот вариант способа рассчитан на низкую бдительность сотрудников организации и лиц, ее охраняющих. При этом преступником может быть использован прием легендирования. Правонарушителями в данном случае являются внутренние пользователи определенной системы. Как видим, эти способы основаны на низкой бдительности сотрудников организации.

2. ***«За хвост» (between the lines entry)*** — это подключение к линии связи законного пользователя и, после прекращения им сеанса связи, продолжение осуществления доступа к системе от его имени. Этот способ съема информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе.

3. ***«Прорыв»*** осуществляется путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор происходит до тех пор, пока на другом конце линии не «отзовется чужой» компьютер). Поскольку в подобном случае один несанкционированный пользователь может быть легко обнаружен, подобный «электронный взлом» осуществляется одновременно с нескольких рабочих мест: в заданное время несколько (более десяти) персональных компьютеров одновременно предпринимают попытку несанкционированного доступа. При таком количестве одновременно атакующих компьютеров даже самые надежные системы защиты от несанкционированного доступа не успевают адекватно отреагировать на созданную нештатную ситуацию. Это может привести к тому, что несколько «атакующих» компьютеров отсекаются системой защиты, а остальные получают требуемый доступ. Один из «прорвавшихся» компьютеров блокирует систему статистики сети, которая фиксирует все попытки доступа. В результате этого другие «прорвавшиеся» компьютеры не могут быть обнаружены и зафиксированы. Часть из них приступает к «взлому» нужного сектора сети, а остальные занимаются фиктивными операциями в целях дезорганизации работы предприятия, организации, учреждения и сокрытия преступления [90, с. 27].

4. ***«Компьютерный абордаж» (hacking)*** обычно используется для проникновения в чужие информационные сети путем перебора идентифицирующих признаков законных пользователей (как правило, имен и паролей). Данный способ совершения компьютерного преступления осуществляется преступником путем случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата.

Иногда для этих целей преступником используется специально созданная самодельная либо заводская (в основном, зарубежного производства) программа автоматического поиска пароля. Алгоритм ее работы заключается в том, чтобы, используя быстродействие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр и специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае совпадения комбинации символов с оригиналом производить автоматическое соединение указанных абонентов.

Стоит обратить внимание на то, что существует множество программ-»взломщиков», называемых на профессиональном языке HACK TOOLS (инструмент взлома). Но эти программы становятся малоэффективными в компьютерных системах, обладающих программой — «сторожем» компьютерных портов. Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора». В этом случае программе-«взломщику» передаются некоторые данные о личности составителя пароля (имена, фамилии, интересы, номера телефонов и т. д.), добытые преступником с помощью других способов совершения компьютерных преступлений. Так как из такого рода данных обычно составляются пароли, эффективность этого метода достаточно высока. По оценкам специалистов с помощью метода «интеллектуального перебора» вскрывается 42 % от общего числа паролей. Интересны результаты экспериментов, проведенные российскими исследователями [91, с. 287], отражающие в указанной ниже таблице 1 процентное соотношение используемых пользователями паролей.

Таблица 1 — **Процентное соотношение используемых пользователями паролей**

№	Тематические группы паролей	% частоты выбора пароля человеком	% вскрываемости пароля
1	Имена, фамилии и производные	22,2	54,5
2	Интересы (хобби, спорт, музыка)	9,5	29,2
3	Даты рождения, знаки зодиака свои и близких; их комбинации	11,8	54,5
4	Адрес жительства; место рождения	4,7	55,0

Продолжение таблицы 1

№	Тематические группы паролей	% частоты выбора пароля человеком	% вскрываемости пароля
5	Номера телефонов	3,5	66,6
6	Последовательность клавиш ПК, повтор символа	14,1	72,3
7	Номер документов (паспорт, удостоверение) и т. д.	3,5	100,0
8	Прочие	30,7	5,7

Подобрав необходимый пароль (для подбора восьмизначного пароля требуется несколько часов), незаконный пользователь получает доступ к компьютерной информации и может проводить с ней любые действия под видом законного пользователя: копировать ее, модифицировать, удалять, заставлять программы производить требуемые операции, например, по переводу денежных средств на свои счета, фальсификации платежных документов и пр.

Примером анализируемого способа неправомерного доступа к компьютерной информации может являться деятельность гр. У, который, находясь в помещении ТОО «Тройка», под предлогом проверки технического состояния ЭВМ дал указание сотруднику З. произвести копирование компьютерной информации с ЭВМ неизвестной фирмы. С этой целью У. продиктовал гр. З. номер телефона, к которому была подключена принадлежащая ЗАО «Вокс» ЭВМ. Гр. З., выполняя указание своего непосредственного начальника У. и в его присутствии, посредством находившегося в помещении ТОО «Тройка» компьютера и подключенного к нему модема, а также данного гр. У телефонного номера, установил компьютерную связь между ЭВМ ТОО «Тройка» и компьютером ЗАО «Вокс». После этого гр. У, руководя действиями гр. З., передал ему так называемый универсальный пароль, позволяющий осуществить доступ к компьютерной информации. Используя этот пароль, гр. З. произвел копирование содержащейся в компьютере ЗАО «Вокс» информации в виде базы данных системных параметров 1-го транкового радиоканала ЗАО «Вокс». В результате произошло копирование и блокирование этой информации, повлекшее нарушение работы ЭВМ ЗАО «Вокс» [92].

5. Другой разновидностью способа получения пароля и кодов доступа является так называемый ***социальный инжиниринг*** («обратный социальный инжиниринг»). Это метод основан на недостаточной бдительности пользователей, когда информация получается в процессе беседы (телефонной, посредством обмена электронными сообщениями) правонарушителя с пользователями системы. При этом способе правонарушитель представляется либо системным администратором, либо сотрудником обслуживающей компьютерной фирмы и запрашивает у собеседника данные о паролях доступа к системе.

6. ***«Неспешный выбор» (browsing).*** Преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в

ее защите. Обнаружив слабые места в системе защиты, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

Обычно такой способ используется преступником в отношении тех, кто не уделяет должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы. Этот способ назван так, потому что поиск слабых мест производится долго и очень тщательно

7. ***«Поиск бреши» (trapdoor entry)*** основан на использовании ошибки или неудачи в логике построения программы путем анализа ее работы. В отличие от «неспешного выбора» при данном способе преступником осуществляется конкурентизация слабых мест в защите компьютерной системы: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены. Появление этого способа обусловлено тем, что программисты иногда допускают ошибки при разработке программных средств, которые не всегда удается обнаружить в процессе отладки программного продукта. Такие ошибки впоследствии может обнаружить только высококвалифицированный специалист. Иногда же программисты намеренно делают такие «бреши» с целью подготовки совершения преступления.

8. ***«Люк» (trapdoor)*** является развитием предыдущего. Когда преступник находит «брешь», он может ввести туда несколько команд. Эти команды срабатывают в определенное время или при определенных условиях, образуя тем самым «люк», который открывается по мере необходимости.

9. ***«Маскарад» (masquerading)*** — проникновение в компьютерную систему, имитируя законного пользователя. Системы защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации (по отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются незащищенными от этого способа. Самый простейший путь к проникновению в такие системы — получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путем подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу. Интересен пример из зарубежной практики: преступник, являющийся законным пользователем компьютерной сети с рабочей станции передал сообщение всем пользователям сервера о том, что его телефонный номер якобы изменен. В качестве нового номера был назван номер собственного персонального компьютера преступника, запрограммированный таким образом, чтобы отвечать аналогично серверу. Пользователи, посылавшие вызов, набирали при этом свой личный код, что предусмотрено правилами электронного обмена информацией. Это обстоятельство и было использовано преступником в корыстных целях. Им был получен исчерпывающий список личных кодов пользователей [93, с. 312].

10. ***«Мистификация» (spoofing)*** используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может

поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени. Пользователь, который подключается к чьей-нибудь системе, обычно уверен, что он общается с нужным ему абонентом. Этим пользуется преступник, который правильно отвечает на вопросы обманутого пользователя. Пока пользователь находится в заблуждении, преступник может получать необходимую информацию (коды доступа, отклик на пароль и т. д.).

11. ***«Аварийный».*** Этот способ совершения компьютерных преступлений характерен тем, что преступник для получения несанкционированного доступа использует программы, которые находятся на самом компьютере. Обычно это программы, которые отвечают за «здоровье» компьютера. Они ликвидируют сбои и другие отклонения в компьютере. Этим программам необходим непосредственный доступ к наиболее важным данным. Благодаря этому преступник может войти в систему вместе с ними.

12. ***«Склад без стен».*** Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.

Также следует отметить, что неправомерный доступ к компьютерной информации может быть связан и с насилием над личностью либо угрозой его применения в целях получения преступниками сведений о способах преодоления средств защиты компьютерной информации и иных данных.

Проиллюстрируем способ и механизм совершения неправомерного доступа к компьютерной информации, где под механизмом преступления следует понимать систему процессов взаимодействия участников преступления как прямых, так и косвенных, между собой и с материальной средой, сопряженных с использованием соответствующих орудий, средств и иных отдельных элементов обстановки [80, с. 12]. Так, например, преступники, делая подборку лиц (вербовали путем подкупа или шантажа) из числа сотрудников определенного банка, для подстраховки завербовали специалиста телефонной станции того населенного пункта, из которого осуществлялось общее управление операцией. В этом населенном пункте на подставное лицо была снята квартира, в которой преступники установили необходимое оборудование. В данной квартире работал главный исполнитель. Помимо него, в разных районах населенного пункта было задействовано еще примерно 10-12 компьютеров с операторами, так как один компьютер не обеспечит эффективного проведения операции. Таким образом, общее число участников преступления составило 30 человек. Однако об ее истинной цели знали не более 5 человек — главный исполнитель и его непосредственные помощники. Остальные участники использовались «втемную» — каждый из них знал лишь о своей конкретной задаче.

Проникновение в компьютерную сеть банка осуществлялось путем опосредованного доступа. При осуществлении преступной деятельности главный исполнитель в период прохождения фиктивных платежных поручений ввел через свой компьютер основное платежное поручение и поставил его первоочеред-

ным на обработку и отправку по указанным адресам. После этого он ввел фиктивные поручения в целях сокрытия основной проводки. Сразу же после оплаты основного платежного поручения была дезорганизована система взаиморасчетов банка со своими клиентами, что на некоторое время полностью парализовало ее [84, с. 27].

Вторая группа. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся по борьбе с экономическими преступлениями. Рассмотрим наиболее широко используемые преступниками способы.

1. ***Подмена данных*** — наиболее простой и поэтому очень часто применяемый способ совершения преступления, который заключается во вводе неверной информации, на основании которой системы автоматизированной обработки информации имеют на выходе неверные результаты. В частности, данный способ применяется для приписывания счету «чужой» истории, т. е. модификация данных в автоматизированной системе банковских операций, приводящей к появлению в системе сумм, которые реально на данный счет не зачислялись. Например, таким способом экономистом областного производственного объединения К. были совершены хищения денежных средств. Как свидетельствуют материалы уголовного дела, будучи экономистом по учету заработной платы и отвечая за достоверность документов и их сдачу, К. на протяжении ряда лет (7 лет) вносила в документы на начисление заработной платы подложные данные. В результате чего заработная плата начислялась на счета вымышленных лиц и переводилась в сберкассы на специально открытые ею счета. Всего таким образом К. похитила 22960 рублей и была осуждена по ч. 1 ст. 91 УК БССР [94, с. 18].

Интересен еще один пример из зарубежной практики. Он заключается в том, что преступнику путем изменения данных в компьютерной системе управления движением грузов по нью-йоркской железной дороге «Пенн-сентрал» удалось похитить 352 железнодорожных вагона с грузами на общую сумму более 1 млн. долларов США. Следствием было установлено, что неизвестным лицом тайно были подменены данные о пунктах назначения грузов, в результате чего они были отправлены по другим адресам и похищены [88, с. 3].

2. ***«Троянский конь» (Trojan horse)*** — тайное введение в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем принимающей «троянского коня» программы, с одновременным сохранением прежней ее работоспособности. Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе либо оказать воздействие на администрацию предприятия с корыстной целью.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вари-

ант увеличения преступниками избыточных сумм на счетах при автоматическом перерасчете остатков денежных средств, связанных с переходом к коммерческому курсу соответствующей валюты. Программа «троянского коня» обнаруживается с большими сложностями только квалифицированными экспертами-программистами. На ее поиск необходимо потратить значительное время.

Из зарубежной следственной практики интересен факт использования «троянского коня» одним американским программистом. Он вставил в программное обеспечение персонального компьютера по месту своей работы команды, которые не выводили на печать для отчета определенные поступления денежных средств. Эти суммы особым образом шифровались и циркулировали только в информационной среде компьютера. Похитив бланки выдачи денег, преступник заполнял их с указанием своего шифра, а затем проставлял в них определенные суммы денег. Соответствующие операции по их выдаче также не выводились на печать и, следовательно, не могли подвергнуться документальной ревизии [93, с. 317].

При этом «троянский конь» имеет свои разновидности:

– «троянская матрешка». Особенность этого способа заключается в том, что это программные модули-фрагменты, которые создают «троянского коня» и самоликвидируются на программном уровне по окончании исполнения своей задачи. Найти эти команды-модули практически невозможно;

– «троянский червь». Особенность этого способа заключается в том, что в алгоритм работы программы, наряду с ее основными функциями, закладывается алгоритм действий, осуществляющих саморазмножения, программное автоматическое воспроизводство «троянского коня». «Программы-черви» автоматически копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети) независимо от других программ. При этом используется тактика компьютерных вирусов, речь о которой пойдет далее.

3. ***Салями (salami attack)*** — присваивание округляемых остатков на счетах. Такой способ совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях. Данный способ основан на методике проведения операций перебрасывания на подставной счет мелочи — результата округления, которая на профессиональном бухгалтерском языке называется «салями».

Данный способ используется, как правило, при хищении денежных средств в тех бухгалтерских операциях, в которых отчисляются дробные (меньше, чем одна минимальная денежная единица) суммы денег с каждой операции, т. к. в этих случаях всегда делается округление сумм до установленных целых значений. Ставка преступников делается на том, что при каждой проверке потерпевший теряет так мало, что это практически не фиксируется документально.

4. ***Логическая бомба (logic bomb)*** — тайное встраивание в программу набора команд, который должен сработать при определенных условиях. Иногда из тактических соображений хищение удобнее всего совершать при стечении каких-либо обстоятельств, которые обязательно должны наступить. Преступни-

ками используется способ совершения преступления, основанный на тайном внесении изменений в программу потерпевшей стороны набора команд, которые должны сработать (или срабатывать каждый раз) при наступлении определенных обстоятельств через какое-либо время. Далее включается алгоритм программы «троянского коня».

Разновидностью «логической бомбы» является временная бомба (time bomb), которая срабатывает по достижении определенного момента времени или временной интервал.

5. ***Подмена кода*** — это, по сути, изменение самого процесса ввода, хранения, обработки, вывода информации.

6. ***Преодоление программных средств защиты***. Это скорей вспомогательный способ совершения преступления, представляющий собой умышленное преодоление системы защиты. Существует несколько разновидностей этого способа:

– *создание копии ключевой дискеты.* Для запускания некоторых систем необходима ключевая дискета, на которой записаны необходимые системные файлы. Преступник может незаконно создать копию такой дискеты с помощью известной программы DISKCOPY. Позже это поможет преступнику попасть в нужную систему;

– *модификация кода системы защиты.* При этом код защиты выполняет в компьютере проверку ключевой дискеты и санкционированности запуска защищенного информационного ресурса. Модифицируя этот код, преступник просто обходит эти функции. То есть происходит обход системы защиты. Данный способ может быть реализован только высококлассным специалистом, имеющим опыт в этом деле. Время обхода системы защиты может исчисляться неделями;

– *снятие системы защиты из памяти ЭВМ.* Система защиты периодически загружает защищаемое программное средство в оперативную память для передачи управления этой программой коду защиты. Когда код еще не взял управление на себя, в оперативной памяти находится совершенно незащищенная программа. Преступнику остается сохранить ее в каком-нибудь файле.

7. ***Копирование.*** Этот способ совершения преступления представляет собой незаконное копирование информации преступником программных средств компьютерной техники. Преступник незаконно копирует информацию на свой физический носитель, а затем использует ее в своих корыстных целях. Этот способ распространен из-за своей простоты. Например: два лица заключают договор на разработку программного средства. Заказчик при этом платит определенную сумму за работу. Исполнитель же просто копирует нужную программу из какого-нибудь источника, выдавая ее за свою, и предоставляет ее заказчику.

8. ***Моделирование.*** Для совершения компьютерных преступлений все более характерным становится использование преступником компьютерного моделирования: моделирования поведения устройства или системы с помощью программного обеспечения. Моделируются те процессы, в которые преступники хотят вмешаться, а также планируемые способы совершения преступления.

Например, в последнее время преступниками с целью ухода от налогообложения все чаще начинает использоваться так называемая «черная» или «двойная» бухгалтерия, основанная на существовании двух одновременно работающих программ автоматизированного бухгалтерского учета с взаимоперетекающими контрольными данными. Одна из них функционирует в легальном режиме, а другая — в нелегальном для проведения незаконных («теневых») бухгалтерских операций.

9. ***Реверсивная модель.*** Эта разновидность способа моделирования заключается в следующем. Создается модель конкретной системы, на которую планируется совершить нападение. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем подбираются максимально приближенные к действительности желаемые результаты. После чего модель совершения преступления «прогоняется» назад, к исходной точке, и преступнику становится ясно, какие манипуляции с входными-выходными данными нужно совершить, чтобы достичь желаемого результата.

Это далеко не исчерпывающий перечень способов совершения компьютерных преступлений данной группы. Очень многие способы довольно трудно описать, так как они поддаются лишь описанию языком программирования и очень часто служат вспомогательными, необходимыми лишь для подготовки и вступления в действия другого способа.

10. ***Асинхронная атака*** состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно. Для понимания этого способа совершения преступлений нужно дать понятие операционной системе. Операционная система — комплекс программных средств, обеспечивающих управление информационными процессами при функционировании компьютерной системы. Главная задача операционной системы — обеспечение максимальной производительности компьютера. Функции: управление, коммуникация, планирование и т. д. Понятно, что такой комплекс программ имеет очень большую структуру, состав, размеры. Разработкой операционных систем занимаются профессиональные группы программистов иногда в течение нескольких лет. Поэтому операционные системы невозможно проверить на полную работоспособность. Искусный преступник может внести коррективы в нужную операционную систему и заставить работать ее в своих корыстных целях. Такие изменения заметить достаточно сложно. Внесенные команды будут выполняться одновременно с командами пользователя.

11. ***Компьютерные вирусы.*** Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера или наносящих ущерб хранимой в компьютере информации. Количество новых программных вирусов постоянно растет.

Формальное определение понятия «компьютерный вирус» до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Первое из них было произнесено студентом Калифорнийского университета Фредом Коуэном в августе 1984 г., который, выступая на одной из конференций,

рассказал про свои опыты с тем, что он назвал «компьютерным вирусом» на основании общих черт с вирусом медицинским. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Дело в том, что дать более-менее лаконичное определение, которое бы четко выделило все вирусы из числа обычных программ, невозможно — оно будет либо чрезвычайно широким (включающим в состав вирусов невирусные программы), либо слишком узким (оставляющим без внимания явно вирусные программы). Поэтому представляется обоснованным дать описание некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором обособленном классе программ.

Прежде всего, *вирус* — специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера. Такая способность является единственным качеством, присущим всем типам вирусов. Нужно отметить, что копии вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать (так называемые полиморфные вирусы [95, с. 63]). В этом случае под копированием следует понимать перенесение в другой файл содержания вируса — его деструктивной функции или иного его проявления, а не его формы — закрепленного набора команд для осуществления этих функций. Такие программы обычно составляются преступниками на языке программирования «ассемблер» и не выдают при своей работе никаких аудиовизуальных отображений в компьютерной системе.

Этот способ совершения компьютерного преступления является ничем иным, как логической модернизацией способа «троянский конь», выполняющего алгоритм типа «сотри все данные этой программы, перейди в следующую и сделай то же самое». Этот способ широко распространен по своему применению. В настоящее время в мире существует уже более 16000 вирусов. Для изучения вирусов создана специальная наука — компьютерная вирусология. Напомним, что в зависимости от способности самовоспроизводиться, вредоносные программы подразделяются на программы-вирусы (самовоспроизводящиеся) и вредоносные программы в узком понимании (не самовоспроизводящиеся).

Для понимания способа совершения преступления все вирусы можно подробно классифицировать по определенным основаниям и разбить их на несколько обобщенных групп. С точки зрения науки — компьютерной вирусологии, вирусы можно разделить на *«вульгарные» и «раздробленные», резидентные и нерезидентные.*

«Вульгарные» и «раздробленные» вирусы. Такое деление произведено по алгоритму строения и обнаружения того или иного вируса. «Вульгарные» вирусы написаны одним блоком и легко обнаруживаются специалистами с помощью специальных антивирусных программ, которые будут представлены позже. Что касается «раздробленного» вируса, то нужно сказать, что такая программа раз-

делена на части. Эти части никак не связаны друг с другом, но они «собираются» при определенных условиях во вполне здоровый вирус. При выполнении своей задачи такой вирус распадается или самоуничтожается.

Резидентные и нерезидентные. Резидентной называется программа, которая по окончании работы оставляет свой код в оперативной памяти компьютера Резидентные вредоносные программы при заражении (инфицировании) компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Оперативная память — это память, предназначенная для исполняемых в данный момент программ и оперативно необходимых для этого данных. Резидентная программа работает параллельно другим программам. И если вирус попадает в оперативную память компьютера, то он фактически заражает все программы, с которыми функционирует параллельно. Резидентный вирус, оставляя свой код в оперативной памяти, возобновляется при каждом включении компьютера. Нерезидентные вредоносные программы не заражают память компьютера и являются активными только во время их непосредственной работы. Они оставляют в оперативной памяти небольшие программы, которые не имеют алгоритма распространения вируса. Такой вирус погибает при выключении компьютера.

Н. Н. Безруков проводит классификацию компьютерных вирусов по следующим основаниям: среде обитания; способу заражения среды обитания; воздействию; особенностям алгоритма [95, с. 24].

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули программ, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах они никогда не получают управление и, следовательно, теряют способность к размножению.

Многие вирусы выявляются не сразу: первое время компьютер «вынашивает инфекцию», «вирус» как бы наблюдает за всей обрабатываемой в системе потерпевшего информацией и может перемещаться вместе с ней. Начиная действовать, вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После чего он возвращает программное управление. Потерпевший ничего не заметит, так как его компьютерная система находится в состоянии «здорового носителя вируса».

Далее происходят нарушения в работе компьютера, степень которых зависит от типа и вида вируса. Большинство вирусов не носят разрушительного характера, так как пишутся программистами-любителями — в таких случаях на экране дисплея начинают опадать или геометрически перемещаться буквы и символы (вирус «листопад», «змейка», «мозаика»), исчезают системные файлы с каким-либо определенным расширением (например, com, bat, exe, txt и т. д.),

либо резко на 180 градусов переворачивается изображение, неожиданно на экране дисплея появляется реклама чего-либо и т. д., и т. п.

Этого не скажешь про другую часть вирусов, которая пишется профессиональными программистами, часто имеющими корыстные цели — в этих случаях происходит нарушение нормального режима функционирования средств компьютерной техники: компьютер отказывается нормально загружаться или не загружается совсем, по неизвестным причинам исчезают из памяти файлы, некоторые программные средства самопроизвольно стираются.

В качестве примера рассмотрим схему работы нерезидентного файлового вируса (в отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы могут быть нерезидентны). При запуске исполняемого файла, содержащего вирус, последний получает управление, производит некоторые действия и передает управление основной программе. При этом он ищет новый объект для заражения — подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла.

Если файловый вирус резидентный, то он установится в память и получит возможность заражать другие файлы и выполнять прочие предусмотренные создателем действия не только во время работы зараженного файла, а вообще пока работает компьютер. Заражая исполняемый файл, вирус всегда изменяет его код, что помогает его обнаружить. При этом не обязательно вносятся изменения в размер (длину) файла, поскольку им используются неиспользуемые участки кода, а также не обязательно меняется начало файла.

Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

Загрузочные (системные) вирусы (поражающие загрузочные секторы машинной памяти). Заражение загрузочными вирусами происходит при загрузке компьютера с носителя машинной информации, содержащего вирус. Вирус может попасть, даже если пользователь просто вставил его в приемное устройство (дисковод) зараженного компьютера и, например, прочитал его оглавление.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Механизм действия загрузочного вируса выглядит следующим образом: при включении компьютера управление передается программе начальной загрузки, которая хранится в постоянном запоминающем устройстве (ПЗУ) компьютера. Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А.

Всякая дискета размечена на секторы и дорожки. Среди секторов есть несколько служебных, используемых для нужд операционной системы (в этих секторах не могут размещаться данные), в том числе и сектор начальной загрузки (boot-sector). Как только активный резидентный вирусом, действующий

в «зараженном» компьютере, обнаружит, что в дисководе появилась не защищенная от записи дискета, он производит следующие действия:

– выделяет некоторую область диска и помечает ее как недоступную операционной системе, например, помечает занятые вирусом секторы как сбойные (bad);

– копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;

– замещает программу начальной загрузки в загрузочном секторе (настоящем) дискеты;

– передает управление операционной системе.

Таким образом, при последующем обращении к дискете на «незараженном» компьютере вирусная программа первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору.

Следует отметить, что, как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы жестких дисков компьютеров («винчестеров»). При этом в отличие от дискет на винчестере имеются два типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки MBR (Master Boot Record — главная загрузочная запись). Если жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов — программа начальной загрузки в MBR и программа начальной загрузки в бут секторе загрузочного диска.

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков. Основное разрушительное действие — шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а, зашифровав половину жесткого диска, сообщает об этом пользователю. Основная проблема при лечении данного вида вируса состоит в том, что недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию или сделать новую запись в главный загрузочный сектор.

По степени воздействия вирусы можно разделить на следующие виды:

– неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

– опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

– очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы можно классифицировать на следующие.

1. Простейшие вирусы паразитического характера, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

2. Вирусы-решикаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

3. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

4. Существуют и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

5. «Паразитические», которые обязательно изменяют программные файлы.

6. «Студенческие» написаны любителями. Такие вирусы содержат много ошибок и легко обнаруживаются специальными программами.

7. Вирусы-невидимки — это достаточно совершенные вирусы, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Их трудно обнаружить антивирусной программой и невозможно увидеть при обычном просмотре файлов, так как при открытии зараженного файла они немедленно удаляются из него, а при закрытии опять заражают.

8. Вирусы-«призраки» — трудно обнаруживаемые вирусы. Дело в том, что они, заражая программы, постоянно меняют свой код (содержание). Так что во всех следующих зараженных программах нельзя заметить какого-то совпадения. Поэтому эти вирусы трудно обнаружить с помощью антивирусных программ, основанных на этом принципе. Этот вид вируса называют также «полиморфный вирус» и на сегодняшний день представляется наиболее опасным. Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите, то есть это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования — имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Представляется, что рассмотренные классификации вирусов применимы и к вредоносным программам в узком понимании.

Вирусы представляют наибольшую опасность. Эта проблема заставляет вирусологов отходить от стандартных антивирусных программ и находить другие методы борьбы с вирусами [96, с. 18].

Существует очень много вирусных модификаций. Можно предположить, что по задуманному преступником и реализованному алгоритму работы вируса можно судить о том, насколько профессионально подготовлен преступник (то есть специалист или «студент», с большим числом ошибок и т. д.). Также необходимо отметить, что способ совершения преступления посредством компьютерного вируса может применяться преступником как самостоятельно, так и в составе комплексных способов. В последнем случае при сочетании этого способа с другими он будет выполнять роль маскирующего фактора в преступлении с целью его сокрытия (как, например, поджог хранилища материальных ценностей после их частичного или полного похищения).

Третья группа, как нами уже было отмечено выше, к ней относятся комплексные методы, под которыми понимается использование преступником двух и более способов, а также их различных комбинаций при совершении преступления. Эти способы были подробно рассмотрены в первых группах. Некоторые из них оказываются вспомогательными, работающими на основной способ, выбранный преступником в качестве центрального, исходя из конкретной преступной цели и ситуации.

В качестве примера комплексного использования способов совершения компьютерных преступлений приведем сведения из зарубежной практики расследования. Так, в конце сентября 1993 г. в г. Москве было совершено покушение на хищение в особо крупных размерах 68 млрд. 309 млн. 768 тыс. руб. из Главного расчетно-кассового центра (ГРКЦ) Центрального Банка России (ЦБР), расследованное следственным управлением ГУВД.

В правоохранительные органы поступила информация о незаконном зачислении на корреспондентский счет коммерческого банка (КБ) «С-вест» денежных средств в размере 10 млрд. 70 млн. 100 тыс. рублей. Предварительной проверкой было установлено, что указанная сумма денег поступила 15 сентября 1993 г. с одного из счетов РКЦ г. Москвы. С этого же счета, в этот же день незаконно были списаны и сразу же зачислены на корреспондентские счета восьми московских коммерческих банков денежные средства на общую сумму 58 млрд. 239 млн. 668 тыс. рублей. В ходе дальнейшей проверки было установлено, что зачисление средств произошло из-за умышленного добавления к массиву входных данных программного комплекса «Операционный день РКЦ» дополнительных записей электронных банковских документов. На умышленность проведенной операции прямо указывает факт несохранения электронных банковских документов за 16 сентября 1993 г., вопреки установленным правилам.

В ходе проведенного следствия выяснилось, что указанные электронные операции преступниками были осуществлены с использованием широко распространенных средств компьютерной техники: ПК моделей «IBM PC/AT-286» и «IJF SUPER 286», печатающих устройств (принтеров) моделей «Citizen» и «HP Desk Jet-500C», дискет и листингов. Один из компьютеров был подключен

через модем к городской телефонной сети и имел зарегистрированный пользовательский номер абонента в лице коммерческой фирмы «П.-Т.». Используя в качестве маскировки способ манипуляции данными, преступниками было произведено дробление указанной выше суммы на неравные долевые части с зачислением на соответствующие счета КБ. Для дальнейшего сокрытия преступления, преступниками был применен следующий прием — они не сразу перевели раздробленные суммы на заранее подготовленные счета, а в течении нескольких часов перекидывали данные суммы по разным счетам клиентов, обслуживаемых ГРКЦ ЦБ России по г. Москве, прогоняли их по цепочкам счетов.

В результате принятых правоохранительными органами мер 15 октября 1993 г. в КБ «С-вест» была предотвращена попытка незаконного получения 10 млрд. 70 млн. 100 тыс. рублей по двум фиктивным платежным документам, подготовленным с использованием средств компьютерной техники [97, с. 44].

1. ***Способ «Перехват»*** представляет собой комплексный метод, направленный на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата (имея также разновидности: физическую и электронную), широко практикуемых в оперативно-розыскной деятельности правоохранительных органов. Следует отметить, что при производстве перехвата средства компьютерной техники будут выступать как в качестве предмета, так и в качестве орудия совершения преступного посягательства.

2. ***Непосредственный (активный) перехват*** осуществляется с помощью непосредственного подключения и телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. Объектами перехвата также могут быть кабельные и проводные системы, системы радио- и спутниковой связи. В связи с этим различают:

1) форсированный перехват, представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

2) перехват символов — выделение из текста, набираемого пользователем на клавиатуре терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;

3) перехват сообщений — несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Подключение осуществляется с помощью использования бытовых средств и оборудования: телефона, отрезка провода, составляющих телефонного кабеля, компьютерного полипроводного шлейфа, зажимов типа «крокодил», специальных щупов-игл от контрольно-измерительной аппаратуры, набора радиомонтажных инструментов, кассетного портативного магнитофона, принтера, модема, либо персонального компьютера типа «Laptop» в блокнотном и субб-

локнотном исполнении. После подключения к каналу связи вся информация записывается на физический носитель или переводится в человекочитаемую форму посредством бытовой или специальной электронной аппаратуры.

В качестве специальной аппаратуры преступниками могут использоваться:

а) компьютеризированные анализаторы проводных линий связи типа «РК-1155», позволяющие одновременно прослушивать до 256 линий связи;

б) многофункциональный цифровой регистратор сигналов типа MSR (Multi Signal Registrator), обычный компьютер, реализованный на базе платформы «Intel» с использованием платы обработки сигналов на основе процессора «ADSP» с 16-канальным автоматическим цифровым преобразователем; он обеспечивает длительный непрерывный перехват речевой, факсимильной и цифровой информации по 4-8-16-32 каналам проводной и радиосвязи (на выбор) с последующей ее автоматической фильтрацией (удалением шумов и фона) распознаванием (идентификацией голоса), обработкой и архивированием.

3. ***Электромагнитный (пассивный) перехват.*** Не всегда перехватывающие устройства требуют непосредственного подключения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации. Электромагнитный перехват осуществляется по остаточным излучениям тех или иных устройств (дисплея, принтера, систем коммуникаций), причем на достаточном удалении от объекта излучения.

Электронно-лучевая трубка излучает в окружающее пространство электромагнитные волны, несущие в себе определенную информацию, данные («электронный смог»). Волны, излучаемые этим прибором, примерно так же, как при телевизионном вещании, проникают сквозь различные физические преграды с некоторым коэффициентом ослабления, например, через стекло оконных проемов и стены строений, а принимать их можно, находясь в соседнем здании помещении. Современные технические средства позволяют снимать и расшифровывать излучения работающего принтера на расстоянии до 150 м, излучения мониторов и соединительных кабелей — до 500 м. Как только эти сигналы приняты соответствующей аппаратурой и переданы на другой компьютер (преступника), можно получить изображение, идентичное изображению, возникающему на мониторе «передающего» компьютера, для чего достаточно настроиться на его индивидуальную частоту. Каждый компьютер можно идентифицировать по конкретным параметрам: рабочей частоте, интенсивности электромагнитного излучения и т. д. Например, для осуществления преступных целей иногда достаточно смонтировать приемную антенну по типу волнового канала и имеющую более острую, несимметричную диаграмму направленности. После чего разработать (или использовать готовую) программу расшифровки «снятых» данных.

Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 г. в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании PTT Вим-Ван-Эк шокировал специалистов тем, что с

помощью разработанного им устройства из своего автомобиля, находящегося на улице, «снял» данные с экрана монитора персонального компьютера, установленного на 8 этаже здания, расположенного в 100 метрах от автомобиля [98, с. 94].

Еще одним примером совершения неправомерного доступа к компьютерной информации подобным способом является дело по обвинению Л. и М.. В ходе расследования было установлено, что М. собственноручно у себя дома произвел демонтаж и переоборудовал заранее приобретенные им сотовые телефоны фирмы «Моторолла» под микропроцессоры со специальной программой. Изготовив таким образом два аппарата с режимом автосканирования и шесть аппаратов с возможностями ввода с клавиатуры скопированных номеров в электронные записные книжки, он осуществлял неправомерный доступ к сети ЭВМ компании сотовой телефонной связи «К-Мобайл». Путем модернизации телефонного аппарата «Моторолла» гр. М. была получена возможность фиксации в радиусе до 200 м абонентского и серийного номера аппарата законного пользователя сотовой телефонной сети с последующим занесением его в память электронной записной книжки. Это позволяло производить телефонные звонки с переделанных таким образом сотовых телефонных аппаратов бесплатно, за счет законных клиентов сотовой сети [99].

При совершении компьютерного преступления указанным способом преступниками используются приемы и методы оперативно-розыскной деятельности, специальная техника, например, сканирующие устройства.

4. ***Аудиоперехват или снятие информации по виброакустическому каналу*** является наиболее опасным и достаточно распространенным. Защита от утечки по этому каналу очень сложна. Этот способ съема информации имеет две разновидности: заходовую (заносную) и беззаходовую.

Заходовая (заносная) заключается в установке инфинитивного телефона (подслушивающего устройства — «таблетки», «клопа», «жучка» и т. п.) в аппаратуру средств обработки информации, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарной сигнализации, электросеть и т. п.), а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента и т. п.).

Установка «клопа» или иной разведывательной аппаратуры на объект возможна тремя способами: 1) необходимо скрытное или легендированное проникновение в помещение; 2) радиопередающая и звукозаписывающая аппаратура устанавливается во время постройки или ремонта помещения; 3) приобретается или заносится самой потерпевшей стороной (монтируется в приобретаемые предметы). В качестве примеров специальной техники можно привести: спецмикрофоны с возможным дистанционным управлением; диктофоны с длительной записью; цифровые адаптивные фильтры типа «АФ-512», «DAC-256» и «DAC-1024», позволяющие проводить обработку зашумленных речевых сигналов. Обнаружить аппаратуру съема информации крайне трудно, т. к. она обыч-

но очень хорошо камуфлируется преступником (под микросхему, зажигалку, булавочную головку и т. д.).

Беззаходовая разновидность наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съема информации устанавливают на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы.

Выделяют следующие типовые конструкции инженерно-технических сооружений: несущие стены зданий, перегородки, перекрытия, окна, оконные рамы, двери и дверные коробки, вентиляционные воздуховоды, трубопроводы. При этом необязательно проникать в помещение — достаточно приблизиться к нему снаружи. Датчик устанавливается либо непосредственно, либо дистанционно. В последнем случае используются различные выстреливающие устройства, предназначенные для дистанционного снятия речевой информации через открытые окна, двери и т. п.

5. ***Видеоперехват*** — заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники. Этот способ имеет две разновидности: физическую и электронную.

В первом случае перехват информации производится с помощью применения преступником различной бытовой видеооптической техники. Этот способ осуществляется как физически, так и электронно. Физически перехват информации производится с помощью применения преступником различной бытовой видеооптической аппаратуры (например, бинокля, прибора ночного видения, оптического прицела и т. п.). При этом преступник проводит отдаленное наблюдение за объектом (жертвой) в целях получения необходимой информации, которую в отдельных случаях фиксирует на физический носитель. В рассматриваемом случае орудие преступления находится непосредственно в руках преступника.

Во втором случае процесс получения информации преступником осуществляется с использованием специальной техники. В данном случае передающее устройство находится непосредственно на объекте наблюдения, а приемное — в руках преступника. Может использоваться следующая спецтехника: спецвидеомагнитофоны с длительной записью; оборудование для скрытой видеосъемки; цифровые электронные видеокамеры; приборы ночного видения и т. п.

Э. Мелик выделяет также в этой группе метод «Уборка мусора», то есть поиск «отходов» информационного процесса, как физического характера, так и электронного [82]. Этот способ совершения преступления заключается в неправомочном использовании преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной.

Физический поиск отходов сводится к обследованию рабочих мест программистов, содержимого мусорных баков, емкостей для технологических отходов для сбора оставленных или выброшенных физических носителей информации, а также обследованию различной документации, оставленной на рабо-

чем месте: ежедневников, книг рабочих записей, перекидных календарей и т. п. в целях поиска черновых записей, паролей доступа в систему и пр.

Электронный вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования средств компьютерной техники. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы.

В некоторых случаях преступником могут осуществляться действия, направленные на восстановление и последующий анализ данных, содержащихся в стертых файлах. Специалисты считают, что для поиска и восстановления программы, «стертой» из памяти компьютера требуется не более 40 минут [95, с. 4]. Достижение этих целей предполагает обязательное использование в качестве орудия преступления различных программных средств специального назначения, относящихся к инструментальным программным средствам. Одним из них является программный комплекс «PC Tools Deluxe», содержащий универсальную программу (pct.exe), позволяющую восстанавливать ранее стертые программы и файлы.

В целях более глубокого понимания механизма совершения преступления в сфере высоких информационных технологий, рассмотрим его на примере входа в сеть с использованием сетевых реквизитов (имени и пароля), принадлежащих другим лицам. Преступление совершается следующим образом. Прежде всего, преступнику необходимо завладеть чужими сетевыми реквизитами. Обычно это происходит по одной из следующих схем.

1. Путем распространения либо предоставления доступа к вредоносной программе типа «троянский конь», замаскированной под другую программу либо документ, пользователь, переписавший и запустивший данный файл, активизирует «вирус», который самостоятельно собирает информацию о реквизитах данного пользователя и пересылает на компьютер злоумышленника.

2. Злоумышленник сам, либо используя одну из программ (например, «Legion»), находит компьютер, работающий в сети, подключается к нему и копирует к себе на диск файл с расширением pwl, содержащий все используемые данным компьютером коды доступа в зашифрованном виде, после чего дешифрует их (например, с помощью программы pwlview.exe).

3. Приобретает у третьих лиц полученные одним из перечисленных ранее способов нужные сетевые реквизиты.

Подведя итог способам совершения преступлений, хотелось бы отметить, что их становится все больше и больше. Это происходит по мере совершенствования средств компьютерной техники. Хочется надеяться, что эта проблема будет глубже изучена отечественной криминалистикой, так как по проведенному исследованию о существовании тех или иных способов совершения компьютерных преступлений знают всего около 10 % респондентов.

Представление же способов совершения преступления невозможно, по нашему мнению, без раскрытия характеристики орудий и средств, применяе-

мых при совершении преступлений в сфере высоких информационных технологий.

Так, в современных условиях бурного развития средств вычислительной техники и периферийного оборудования орудия и средства совершения неправомерного доступа к компьютерной информации постоянно модернизируются и совершенствуются. При исследовании указанного элемента, учеными выдвигались несколько точек зрения по данному вопросу. Так, по мнению Д. А. Вечерского и И. И. Шалькевич [52, с. 27], все применяемые орудия и средства, можно разделить на:

– общетехнические (монтажные инструменты, шлейфы, зажимы, щупы, контрольно-измерительная аппаратура, записывающие устройства, устройства прослушивания, встраиваемые в аппаратуру обработки информации (т. н. «жучки»), устройства для регистрации электромагнитного излучения и т. д.);

– специфические компьютерные, которые подразделяются на аппаратные (компьютеры и компьютерная техника, периферийные устройства (модемы, сетевые карты, цифровые видеокамеры и т. п.)) и программные (система команд, или мнемокодов, или управляющих информационным процессом данных, на основании которых происходят те или иные манипуляции с машинной информацией). Они могут вообще не иметь материального воплощения, будучи используемы как информация в «чистом» виде. Для воздействия на объект атаки преступник может использовать как стандартное, свободно распространяемое программное обеспечение (в этом случае результаты такого воздействия предсказуемы и достаточно легко подвергаются анализу) либо специально разработанные им программы.

Ю. М. Гаврилин и ряд его соратников, под орудиями совершения преступлений в сфере компьютерной информации понимают средства компьютерной техники, в том числе и специальное программное обеспечение. Ими предлагается различать средства непосредственного и опосредованного (удаленного) доступа [75, с. 74].

К орудиям непосредственного доступа они относят машинные носители информации, а также все средства преодоления защиты информации. Причем отмечают, что каждой категории средств защиты (организационно-тактических, программно-технических) соответствует свой набор орудий неправомерного доступа к компьютерной информации. Например, при получении информации с компьютера, находящегося в охраняемом помещении, преступникам необходимо изготовить пропуск, выяснить пароль входа в систему, при необходимости применить различные электронные ключи, личные идентификационные коды и пр. В таких случаях может задействоваться и различное периферийное оборудование (принтер, CD-ROM — накопитель, стример, дисководы), а также носители компьютерной информации (дискеты, лазерные диски, кассеты с магнитной лентой для стримера).

К орудиям опосредованного (удаленного) доступа относят сетевое оборудование (при неправомерном доступе из локальных сетей), а также средства доступа в удаленные сети (средства телефонной связи, модем).

А. В. Кузнецов и Ю. М. Гаврилин отмечают, что одним из орудий неправомерного доступа к компьютерной информации является сам компьютер [75, с. 76]. Этим в значительной степени объясняется и сложность расследования данного вида преступления. Связано это с тем, что идентифицировать компьютер, с помощью которого был осуществлен неправомерный доступ, практически невозможно. Да и сам поиск такого компьютера может привести к разрушению ряда других программ и причинению крупного материального ущерба. К тому же преступники, будучи квалифицированными специалистами, продумывают и надежные способы сокрытия совершаемого преступления.

Одним из распространенных средств совершения неправомерного доступа в последнее время стала глобальная мировая телекоммуникационная сеть Интернет. Здесь показательно уголовное дело по обвинению гр. Ш., который, находясь в своей квартире, с помощью своего компьютера вошел в персональный компьютер, принадлежащий магазину, занимающейся продажей компьютерной техники, расположенный в глобальной информационной сети Интернет, выдал себя за держателя кредитной карты, заказал компьютерное оборудование на общую сумму 5900 долларов США и получил его на складе в г. Алматы [100].

Приведенные выше точки зрения, по нашему мнению, смешивают понятия орудия и средства совершения преступлений, что ведет, как отмечает У. К. Кошанов, к «непомерному расширению объема понятий орудий преступления, так и функциональному назначению охватываемых ими предметов» [101, с. 15].

Полагаем, что под орудием преступления следует понимать то, с помощью чего непосредственно осуществляется преступление (например, мошенничество, где обман совершается с непосредственным использованием компьютера — в ходе переписки — без применения специальных программ; звукозаписывающая аппаратура — при совершении аудиоперехвата или снятия информации по виброакустическому каналу), а под средствами — объекты и предметы, с помощью которых лицо достигает целей преступного деяния (программы-вирусы, сети электросвязи, компьютерные системы). В соответствии с Законом Республики Казахстан «О связи» от 13 мая 1999 г., под сетями электросвязи понимаются технологические системы, обеспечивающие один или несколько видов передачи: телефонную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и другие виды радио- и проводного вещания [102].

Данное разделение позволит также более точно квалифицировать в уголовно-правовом аспекте совершаемые преступные деяния (например, неправомерный доступ к компьютерной информации; создание вредоносных программ для ЭВМ; внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению информации; собирание сведений, составляющих коммерческую или банковскую тайну, путем перехвата в средствах связи и т. д.).

Вышеизложенное свидетельствует о том, что понятие «компьютер» используется практически во всех высказываниях и определениях, однако в целях устранения различного толкования данного понятия полагаем необходимым

обратиться к исследованию А. В. Сырбу, в котором, на наш взгляд, достаточно всесторонне исследован понятийный аппарат компьютерных систем, компьютерной техники и компьютерной информации. Так, под компьютером (персональным компьютером (ПК), ЭВМ) понимается комплекс электронных устройств, позволяющих производить предписанные программой и пользователем операции (сбор, накопление, хранение, обработку, выдачу информации, включая передачу ее по телекоммуникационным сетям и тому подобное) над символьной и образной информацией и через установленные каналы выходить в информационно-вычислительную сеть, а также к источникам массовой информации. Компьютер состоит из системного блока, устройств ввода-вывода (клавиатура, монитор) и дополнительных устройств (модем, принтер, мышь, световое перо, микрофон, стример, сканер, плоттер и др.) [23, с. 49-50].

Хотелось бы отметить, что данное нами разграничение не претендует на роль исключительного и в дальнейшем может быть совершенствовано. Однако, отсутствие на сегодняшний день нормативно-правового закрепления указанных элементов, побудило нас к исследованию в данном вопросе, который, может являться темой самостоятельного диссертационного исследования уголовно-правовой квалификации компьютерных преступлений.

Следующим элементом криминалистической характеристики, рассматриваемым нами, является характеристика обстановки, места и времени совершения преступлений в сфере высоких информационных технологий.

Так, под обстановкой совершения преступления понимается система различного рода взаимодействующих между собой до и в момент преступления объектов, явлений и процессов, характеризующих место, время, вещественные, природно-климатические, производственные, бытовые и иные условия окружающей среды, особенности поведения непрямых участников противоправного события, психологические связи между ними и другие факторы объективной реальности, определяющие возможность, условия, обстоятельства совершения преступления [103, с. 15], то есть, все окружающие субъекта условия, в которых осуществляется преступная деятельность, что имеет существенное значение для анализа преступного деяния.

В. И. Куликов разделил эти условия на три категории: природные (природные вещества, явления, условия и процессы), техногенные (вещества, вещи, предметы, процессы, создаваемые или используемые человеком в процессе трудовой или иной деятельности, в быту и т. д.), социально-психологические (отношения в трудовых коллективах, семье и т. д.) [103, с. 15]. Такой подход в целом поддерживает В. А. Образцов, однако при этом он отмечает, что с логической точки зрения продукты человеческой деятельности и социально-психологические факторы относятся к частям одной системы, называемой социальной средой. В соответствии с этим условия, характеризующие обстановку совершения преступления, он подразделяет на природно-климатические и условия социальной среды [104, с. 12].

Обстановка совершения преступлений в сфере высоких информационных технологий, на наш взгляд, характеризуется также дополнительными фактора-

ми. Прежде всего, следует указать, что эти преступления совершаются в области профессиональной деятельности. Преступники, как правило, владеют не только специальными познания и навыками в узкой предметной профессиональной области устройств ЭВМ и программного обеспечения, но и специальными знаниями в области обработки информации в информационных системах в целом. При этом им необходимы специальные познания в соответствующих финансовых, банковских и подробных информационных технологиях.

Все эти преступления всегда связаны с наличием и состоянием средств защиты компьютерной техники (организационных, технических, программных), сложившейся на объекте дисциплины, требовательностью со стороны руководителей к соблюдению норм и правил информационной безопасности и эксплуатации ЭВМ и т. п.

Особенностью данного рода преступлений является то, что на их совершение практически не оказывают влияние природно-климатические факторы.

Обстановка совершения компьютерного преступления способна влиять на формирование всех остальных элементов криминалистической характеристики преступления рассматриваемой категории, определять особенности поведения преступника и потерпевшей стороны.

Наиболее важным компонентом обстановки подготовки, исполнения и сокрытия преступления в данном случае являются специфические условия деятельности потерпевших сторон (физических и юридических лиц), которые можно разграничить на:

1. Объективные:

– вид деятельности или род занятия (сфера деятельности — хозяйственная, коммерческая, управленческая, производственная, информационная, посредническая, финансовая, топливно-энергетическая, транспортная, услуги и т. д.);

– форма собственности предприятия или физического лица, правовой режим отдельных видов имущества, в т. ч. информации и информационных ресурсов;

– назначение и структура организации производственного процесса, характер потребляемых ресурсов и выпускаемой продукции (в т. ч. и интеллектуальной);

– система учета и отчетности;

– кадровое и материально-техническое обеспечение;

– вид используемых СВТ, связи и телекоммуникаций, их тактико-технические данные и конструктивное несовершенство;

– наличие необходимых помещений и оборудования;

– порядок отпуска и реализации продукции, ценностей;

– наличие и техническое состояние средств учета, защиты информации, охраны и т. д.;

2. Субъективные, к которым относятся факторы социально-психологического и организационно-управленческого характера как:

– отступление от технологических режимов обработки информации, правил производства, проведения пусконаладочных, ремонтных, регламентных (техническое обслуживание) работ, эксплуатации СВТ, а также учета, хранения, распределения и расходования ценностей;

– несовершенство этих правил;

– отсутствие или несовершенство средств защиты информации;

– нарушение правил работы с охраняемой законом компьютерной информацией;

– необоснованность использования СВТ в конкретных технологических процессах и операциях;

– неудовлетворительная организация производственных процессов, наличие одновременно ручных и автоматизированных этапов обработки документов;

– психологически неправильные межличностные взаимоотношения руководителей с подчиненными и другими работниками и т. д.

Изложенное позволяет утверждать, что выявление особенностей сложившейся обстановки позволяет быстрее определить, на что следует обратить особое внимание при осмотре места происшествия, изучении компьютерного оборудования и документов, вызове и допросе свидетелей и решении вопросов о необходимости изъятия определенных документов и т. п.

Местом совершения преступлений в сфере высоких информационных технологий являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в каком-либо технологическом процессе.

Особенностью совершения преступлений в сфере высоких информационных технологий является то, что место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать. Причем это бывает практически при каждом случае опосредованного (удаленного) доступа к компьютерной информации. При непосредственном же доступе место совершения противоправного деяния и место наступления вредоносных последствий совпадают. В этой связи можно говорить о том, что преступления в сфере высоких технологий имеют транснациональный характер, то есть преступление совершается в одной стране, а негативные последствия наступают в другой. При этом если неправомерный доступ предпринимается одновременно с нескольких компьютеров, то количество мест совершения преступления соответствует числу используемых при этом компьютеров.

Ярким примером этому может служить одно из уголовных дел, расследование которого осуществлялось российскими правоохранительными органами в тесном контакте с правоохранительными органами США. Возбуждено оно было в отношении В. Левина — гражданина Российской Федерации, 13-ти рус-

ских с иностранным подданством, а также гражданина Нидерландов, которые вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих «City Bank of America», расположенному в Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 1994 г., используя компьютерную систему телекоммуникационной связи Интерент и преодолев семь рубежей многоконтурной защиты от несанкционированного доступа, с помощью персонального компьютера из офиса АО «Сатурн», находящегося в г. Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих действий преступники осуществили около 40 переводов денежных средств на общую сумму 10 млн. 700 тыс. 952 доллара США со счетов клиентов названного банка, находящихся в 10 странах мира (США, Канаде, Мексике, Аргентине, Новой Зеландии, Арубе, Колумбии, Гонконге, Индонезии, Уругвае), на счета лиц, входящих в состав преступной группы и проживавших в 7-ми других странах (США, Финляндии, Израиле, Швейцарии, Германии, России и Нидерландах) [105, с. 10].

Местом, где в результате совершения рассматриваемого преступления наступил преступный результат, являются предприятия, организации, учреждения различных форм собственности, имеющие информацию на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети, т. е. преимущественно те, в которых используются высокие технологии.

Значительное количество банков, пенсионных фондов часто сталкиваются с проблемой защиты персональных данных вкладчиков. Острой является и проблема защиты сведений, хранящихся в паспортно-визовой службе, о регистрации по месту жительства отдельных категорий граждан, это связано с тем, что преступники проявляют большой интерес к местам хранения и учета сведений о регистрации граждан по месту жительства одиноких, престарелых граждан, а так же алкоголиков, наркоманов и пр.

Можно выделить следующие предприятия, учреждения, организации (различных форм собственности), в которых рассматриваемое преступление может быть совершено работающими там лицами.

1. Предприятия, организации, учреждения, фирмы, компании с обширной организационной структурой, где властные полномочия сконцентрированы, а ответственность обезличена. «В связи с компьютеризацией все большее участие в управленческой деятельности принимают люди, имеющие отношение к программному обеспечению и базам данных автоматизированных информационных систем. Большинство же руководителей не имеют полного представления о том, как же эти системы функционируют. Тем самым создаются предпосылки для несанкционированного их использования теми сотрудниками, которые решили встать на путь преступления» [106, с. 21].

2. Предприятия, организации, учреждения, фирмы, компании, имеющие высокие темпы развития, за которыми не успевают управленческие функции. В некоторых случаях сами руководители не знают с чего начать, какие организа-

ционно-управленческие мероприятия необходимо провести, чтобы исключить неправомерный доступ к компьютерной информации.

3. Предприятия, организации, учреждения, фирмы, компании, которые сворачивают свою деятельность. «Их ресурсы настолько ограничены, что (на фоне вынужденного отказа нанимателя от услуг целого ряда лиц, возбуждения при этом негативных эмоций) создает предпосылки противоправных действий» [106, с. 22].

4. Предприятия, организации, учреждения, фирмы, компании, созданные с привлечением иностранного капитала (различные совместные предприятия), имеющие устойчивые связи с аналогичными зарубежными фирмами, поддерживающими устойчивые деловые отношения с ближним и дальним зарубежьем. Зарубежные исследователи называют предприятия, созданные с участием иностранного капитала, «зоной повышенной криминальной опасности».

5. Предприятия, организации, учреждения, фирмы, компании, где в силу различных обстоятельств царит ненормальный морально-психологический климат, например, из-за обид лиц, находящихся на самом низу социальной лестницы, по поводу своего приниженного положения по сравнению с другими (оплата труда, предоставление льгот). Это относится и к случаям, когда в самом руководстве фирмой, компанией нет единства взглядов, в силу чего менеджеры высокой квалификации принимают решение оставить фирму и открыть собственный бизнес. В этой связи представляют интерес обобщенные сведения о потерпевшей стороне, указанные профессором Е. Р. Россинской. Рассматривая все преступления в сфере компьютерной информации в целом, она подразделяет потерпевших на три основные группы: собственники компьютерной системы, клиенты, пользующиеся их услугами, иные лица [107, с. 88].

Следует отметить, что неправомерный доступ к компьютерной информации, как правило, осуществляется в:

1) служебных помещениях самого предприятия (организации), где установлен компьютер или группа компьютеров (в случае непосредственного доступа к компьютерной информации);

2) жилых помещениях, помещениях других предприятий или организаций, заранее арендованных помещениях, специально оборудованных автомобилях и т. п. (при осуществлении опосредованного — удаленного доступа к компьютерной информации).

Распространение вредоносных программ преимущественно осуществляется в сети Интернет, на рынках, в специализированных магазинах и торговых точках, по месту жительства преступника или потерпевшего или в иных местах.

Время совершения преступления зависит от способа его совершения и объекта, где расположена компьютерная техника. Так, при опосредованных и смешанных способах совершения преступления, связанных с использованием компьютерных сетей и, прежде всего, сети Интернет, преступники выбирают вечерние и ночные часы (с 20.00 до 6.00). Это объясняется тем, что в указанное время тарифы фирм-провайдеров по доступу в сеть ниже, чем днем, а также меньше нагрузка на сети, соответственно выше скорость обмена данными.

При способах совершения преступлений, связанных с непосредственным доступом к компьютерной информации, время определяется режимом работы объекта, где расположена компьютерная техника, то есть это рабочие часы с 9.00 до 18.00.

Время совершения рассматриваемой категории преступлений лишь в относительно редких случаях устанавливается с точностью до дня и очень редко — до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

На сегодняшний день, большой криминалистической проблемой является характерное для большинства фактов покушения на целостность и конфиденциальность информации, разнесение в пространстве и во времени совершение преступления и наступление общественно-опасных последствий. Криминалистические методы расследования и раскрытия этих видов преступной деятельности могут быть эффективными только в случае активных оперативно-следственных мероприятий, проводящихся на межрегиональном уровне в пределах одной страны и на межгосударственном уровне — когда преступники использовали средства международного информационного обмена. В силу указанных пространственно-временных факторов возникает и сложная для решения проблема доказывания причинной связи между действиями лица и наступившим результатом. Поэтому, на наш взгляд, необходимо перейти к раскрытию характеристики личности преступника.

Криминалистическая характеристика преступлений в сфере высоких информационных технологий отличается от уже известных преступных посягательств определенной спецификой. В первую очередь в нее должны входить криминалистически значимые сведения о личности правонарушителя, мотивации и целеполагании его преступного поведения, типичных способах, предметах и местах посягательств, а также о потерпевшей стороне.

Данные о личности преступника в настоящее время базируются на двух специфических группах информации. Первая включает в себя данные о личности неизвестного преступника как по оставленным им следам, так и по другим источникам с целью установления и приемов его розыска и задержания. Такая информация дает представление об общих свойствах какой-то группы лиц, среди которых может находиться преступник.

Вторая же группа включает в себя информацию, полученную с помощью изучения личности задержанного подозреваемого или обвиняемого с целью оценки личности субъекта. Такое разделение на группы данных помогает впоследствии выделить типовые модели категорий преступников, каким-то образом провести типизацию преступников.

Выделение типовых моделей разных категорий преступников, знание основных черт этих людей позволяет оптимизировать процесс выявления круга

лиц, среди которых целесообразно вести поиск преступника и точнее определить способы установления и изобличения конкретного правонарушителя.

Однако прежде чем разграничить преступников на определенные категории, полагаем необходимым дать общую характеристику «компьютерного преступника», а уже затем, исходя из специфики его личностно-психологических качеств и характера преступных деяний, классифицировать в определенные группы.

Зарубежный опыт свидетельствует, что сам факт появления преступлений в сфере высоких информационных технологий в обществе, многие исследователи отождествляют с появлением так называемых «хакеров» (англ. «hack» — рубить, кромсать) — пользователей вычислительной системы (обычно сети ЭВМ), занимающихся поиском незаконных способов получения несанкционированного доступа к данным с их несанкционированным использованием в корыстных целях. Кроме указанных выше «хакеров» компьютерных правонарушителей называют также «крэкерами» и «фрэкерами». Эти названия произошли от соответствующих английских слов «cracker» и «phracker», первое из которых обозначает пользователя ЭВМ, системы ЭВМ или их сети, занимающегося «взломом» (модификацией, блокированием, уничтожением) программно-аппаратных средств защиты компьютерной информации, охраняемых законом, второе — субъекта, специализирующегося на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации.

Данные лица обычно обладают достаточно высокими специальными познаниями и практическими навыками в области новых компьютерных технологий. Как правило, это увлеченные компьютерной техникой школьники, студенты и молодые специалисты, совершенствующиеся на этом виде деятельности. Из публикаций, характеризующих этих лиц, следует, что хакер — очень способный молодой человек, работающий за дисплеем по 12-16 часов подряд, до полного изнеможения, питается урывками. Внешний вид свидетельствует о том, что он не обращает внимание на внешний вид и не слишком интересуется мнением окружающих: джинсы, мятая рубашка, нечесаные волосы. Блестяще знает все подробности операционной системы, языка ассемблер и особенности периферийного оборудования [108, с. 11].

Их деятельность направлена на получение доступа к компьютерной информации, для чего они используют различные способы «взлома», обхода защиты и проникновения в сеть, в результате они похищают и заменяют данные, модифицируют файлы, блокируют работу сети и выводят из строя программное обеспечение. В этих целях они используют различные технические средства, в частности, специальное диагностическое оборудование, поставляемое вместе с оборудованием сети и предназначенное для поиска «слабых мест» в системе ее защиты, средства автоматического проникновения одновременно в несколько включенных в сеть компьютеров.

У одних основная продукция — маленькие недокументированные системные программы. Обычный метод их создания — «кромсание» чужих программ. После некоторых переделок в текст обычно вставляется экзотическое собствен-

ное прозвище. Цель деятельности — создание суперпрограммы (операционной системы, игры, вируса, антивируса, языка программирования и т. п.), которая может «все».

Для других сверхзадача — проникновение в какую-нибудь систему, снятие защиты этой системы или с иного программного продукта.

Третья группа, иногда называемая «информационные путешественники», специализируется на проникновении в чужие компьютеры и сети.

Четвертая группа — создатели троянских программ и компьютерных вирусов. Впрочем, этих уже нельзя назвать хакерами, так как «неформальный кодекс» хакеров запрещает использование своих знаний во вред пользователям.

Объектом посягательства хакеров в большинстве случаев являются:

1) коммерческие или тестовые (отладочные) версии различных программ, выпускаемых фирмами-разработчиками (компьютерные игры, прикладные программы, интегрированные программные пакеты, операционные системы и др.);

2) компьютерные системы, используемые для различных исследований;

3) Web-страницы пользователей сети Интернет (их изменение или замена на другие, изменение адресов электронной почты).

У хакеров есть свои принципы [107, с. 54]. Их этика основана на следующем:

а) компьютеры — инструмент для масс. Они не должны быть собственностью только богатых;

б) информация принадлежит всем. Большинство хакеров начинали с университетской скамьи. Задача университета — создавать и распространять знания, а не держать их в секрете. Хакеры придерживаются этого взгляда независимо от того, являются ли они студентами;

в) программный код — общее достояние. Хорошим кодом должны пользоваться все; плохой код должен быть исправлен, программы не должны быть защищены авторским правом или снабжены защитой от копирования;

г) программирование — это искусство;

д) компьютер — живой организм. За ним нужен уход, им нужно дорожить.

Большинство хакеров — молодые люди в возрасте от 16 до 25 лет, преимущественно мужчины, хотя количество женщин-хакеров растет. В этом возрасте способность к восприятию информации наиболее высока, что особенно важно для компьютерных преступлений. Кроме того, в этом возрасте молодые люди активно ищут пути самовыражения, при этом одни начинают писать стихи, другие уходят из дома, третьи погружаются в мир компьютерных сетей.

В последнее время получила распространение точка зрения, что хакеры образуют свою особую субкультуру, наподобие объединения рокеров, металлистов, панков и пр. [109, с. 104]. Носители этой субкультуры со временем претерпевают серьезную психологическую трансформацию, связанную со сменой ценностных ориентацией. Эта трансформация вызвана тем, что объективной реальностью для хакера является компьютерная сеть — основная среда их обитания. Настоящая объективная реальность для них скучна и неинтересна, однако биологически необходима.

Как правило, хакеры объединены в региональные группы, издают свои электронные средства массовой информации (газеты, журналы, электронные доски со срочными объявлениями и пр.), проводят электронные конференции, имеют свой жаргонный словарь, который постоянно пополняется и распространяется с помощью компьютерных бюллетеней. В таких « литературных» источниках имеются все необходимые сведения для повышения мастерства начинающего хакера — методики и способы проникновения в конкретные системы и взлома систем защиты. Отечественные хакеры тесно контактируют с зарубежными, обмениваются с ними опытом по глобальным телекоммуникационным каналам электросвязи.

Члены хакерских группировок действуют по принципу разделения труда. Группу возглавляет лидер, имеющий, как правило, своих заместителей (координаторов). Лидер осуществляет общее управление, ставит задачи, разрабатывает стратегию существования и развития группы. Заместители занимаются своими направлениями в четко функционирующем механизме; рядовые члены выполняют приказы координаторов и лидера, специализируясь на определенном этапе «производственного процесса».

В такой структуре может присутствовать еще одна ступень — поставщики, которые поставляют хакерам особую информацию: идентификаторы и пароли для доступа в компьютерную сеть, методы обхода или нейтрализации систем безопасности, имеющиеся в них по небрежности или умыслу разработчиков «люки», «дыры» и другие слабые места. Обычно это сотрудники тех или иных фирм, недовольные своим служебным и (или) материальным положением. При этом предоставление информации может носить как разовый, так и долговременный характер.

Сфера интересов хакеров достаточно разнообразна. Известен случай, когда, подключившись к ЭВМ одного западноевропейского военного ведомства, студенты получили возможность повышать людей в звании, назначать на новые должности с баснословным жалованием и т. п. [93, с. 495].

В настоящее время крупные компании стремятся привлечь наиболее опытных хакеров на работу с целью создания систем защиты информации и компьютерных систем.

Обобщая изложенное, приведем примерный портрет субъекта неправомерного доступа к компьютерной информации — лицо мужского пола (хотя количество женщин, совершающих компьютерные преступления, с каждым годом возрастает), высококлассный специалист-программист, профессионал с большим опытом работы, являющийся незаурядной, неординарной личностью, готов принять вызов, настроен на соперничество и противоборство, боится разоблачения, потери уважения, его поведение несколько отклоняется от принятых в обществе норм; он пользуется доверием по службе и имеет свободный доступ к компьютерным системам; как правило, приходит на работу первым, а уходит с нее последним, практически никогда не берет отпуск. Свои действия объясняет тем, что считает их не чем иным, как игрой. Все вышеперечисленное можно считать собирательным понятием «компьютерного преступника».

Для выдвижения версий, базирующихся на основе изучения обнаруженных следов, необходимы также данные и о видах преступников, совершающих подобные преступления. Обобщение отечественного и зарубежного опыта показывает, что преступления в сфере высоких информационных технологий относятся к числу преступлений в области профессиональной деятельности. Из этого следует, что лица, их совершающие, как правило, обладают набором профессиональных навыков по обработке информации с помощью информационных технологий. Классификация субъектов неправомерного доступа к компьютерной информации, предложенная В. В. Крыловым [110, с. 489], в качестве основания которой взят уровень профессиональной подготовки и социальное положение достаточно полно отражает мотивы совершения данного преступления. В соответствии с этим автор выделяет следующие их виды:

а) «хакеры» — лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций;

б) «шпионы» — лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях;

в) «террористы» — лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия;

г) «корыстные преступники» — лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод;

д) «вандалы» — лица, взламывающие информационные системы для их разрушения;

е) психически больные лица, страдающие новым видом психических заболеваний — информационными болезнями или компьютерными фобиями. Эта категория заболеваний связана с нарушениями в информационном режиме человека под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного свойства.

Помимо профессиональных взломщиков компьютерных сетей и программ, в числе лиц, совершающих преступлений в сфере высоких информационных технологий, выделяют лиц, не обладающих серьезными познаниями в области программирования и компьютерной техники, имеющих лишь некоторые пользовательские навыки работы с ЭВМ. Как правило, их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации (например, если компьютер не имеет пароля доступа или пароль известен широкому кругу лиц).

Хотелось бы еще остановиться на одном любопытном факте, который необходимо, на наш взгляд, учитывать при расследовании преступлений в сфере информационных технологий относительно лиц, страдающих новым видом психических заболеваний — информационными болезнями или компьютерными фобиями. Хорошо известно, что многие так сказать «традиционные» преступления совершаются в состоянии алкогольного или наркотического опьяне-

ния. Существует достаточное количество методических руководств, алгоритмов по проведению операций, по предотвращению преступлений. Однако, мало кому известно, что существует понятие «информационной наркомании» («internet-addiction», «pathological internet use»). В сети Интернет практически открыто предлагаются специально созданная музыка («psychedelic music»), компьютерные программы («psychedelic software»), способные вызвать у человека состояние наркотического опьянения. Складывается парадоксальный факт. Если человек распространяет наркотик традиционным путем, то против него может быть возбуждено уголовное дело по соответствующей статье уголовного кодекса, а аналогичное деяние, совершаемое в Интернете по распространению «информационных» наркотиков, остается безнаказанным. Точнее, тоже может быть возбуждено уголовное дело по соответствующим статьям уголовного кодекса, но вся беда в том, что большинство сотрудников правоохранительных органов даже не знают о возможностях деструктивной информации. А ряд сект (взять хотя бы для примера «Белое Братство») умело пользуются возможностями современных информационных технологий воздействовать на сознание и подсознание человека.

Проблема Интернет-наркомании стала реальностью. Интернет-наркомания подобно хроническому алкоголизму или азартной игре имеет разрушительные последствия на человека, его семью, работу, учебу, а в некоторых случаях провоцирует на преступления. По мнению профессора Питсбургского университета Кимберли Янг, проблема Интернет-наркомании в США достигла эпидемических размеров, причем число наркоманов («сетеголиков») продолжает расти. В международную классификацию психических расстройств внесено заболевание «кибернетические расстройства» [111]. Собственно говоря, в сети Интернет имеется практически открытая информация по изготовлению синтетических наркотиков, но это отдельная тема для изложения. Можно только отметить, что методы синтеза наркотиков часто берутся из Интернета.

Классификация личности субъектов компьютерных преступлений имеет определенную специфику. Лица, совершающие подобные преступления, разграничиваются различными учеными на категории группы. Так, исследуя данные о личностных свойствах субъектов преступлений в сфере компьютерной информации, ряд ученых разделяют следующие категории граждан [75, с. 87]:

1. Лица, состоящие в трудовых отношениях с предприятием, организацией, учреждением, фирмой или компанией, где совершено преступление (они составляют более 55 %), а именно:

– непосредственно занимающиеся обслуживанием ЭВМ (операторы, программисты, инженеры, персонал, производящий техническое обслуживание и ремонт компьютерных систем или обслуживающий компьютерные сети);

– пользователи ЭВМ, имеющие определенную подготовку и свободный доступ к компьютерной системе;

– административно-управленческий персонал (руководители, бухгалтеры, экономисты и т. п.).

2. Граждане, не состоящие в правоотношениях с предприятием, организацией, учреждением, фирмой или компанией, где совершено преступление (около 45 %). Ими могут быть:

– лица, занимающиеся проверкой финансово-хозяйственной деятельности предприятия, и др.;

– пользователи и обслуживающий персонал ЭВМ других предприятий, связанных компьютерными сетями с предприятием, на котором совершено преступление;

– лица, имеющие в своем распоряжении компьютерную технику (в том числе владельцы персональных ЭВМ, тем или иным образом получившие доступ к телекоммуникационным компьютерным сетям).

Зарубежные специалисты подразделяют представляющий опасность персонал на категории в соответствии со сферами деятельности [112]:

– операционные преступления — совершаются операторами ЭВМ, периферийных устройств ввода информации в ЭВМ и обслуживающими линии телекоммуникации;

– преступления, основанные на использовании программного обеспечения, — обычно совершаются лицами, в чьем ведении находятся библиотеки программ, системными программистами, прикладными программистами, хорошо подготовленными пользователями;

– для аппаратной части компьютерных систем опасность совершения преступлений представляют: инженеры-системщики, инженеры по терминальным устройствам, инженеры-связисты, инженеры-электронщики;

– сотрудники, занимающиеся организационной работой: управлением компьютерной сетью, руководством операторами, управлением базами данных, руководством работой по программному обеспечению;

– разного рода клерки, работники службы безопасности, работники, контролирующие функционирование ЭВМ;

– специалисты-сотрудники в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих — системные администраторы и другие сотрудники служб автоматизации банков.

Исследуя многочисленные виды преступников в сфере высоких информационных технологий, следует отметить, что их многообразие, исходя из специфики поведения, может и будет увеличиваться пропорционально развитию самих высоких технологий. На наш взгляд, необходимо по ряду оснований выделить их в самостоятельные, обособленные группы, анализ которых позволит выработать систему правовых норм по квалификации совершенных ими деяний, а также методику расследования и раскрытия преступлений, совершенных

определенной группой преступников. В данной ситуации, по нашему мнению, предложенная В. А. Минаевым и В. Н. Саблиным трех элементная классификация, отвечает предъявляемым требованиям [113].

В целом, соглашаясь с предложенной классификацией, полагаем необходимым дополнить ее отдельными позициями. Окончательный вариант разделения преступников в сфере высоких информационных технологий на три основные группы представлен в следующем виде.

К *первой группе* преступников можно отнести лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей.

Они весьма любознательны, обладают незаурядным интеллектом. При этом не лишены некоторого своеобразного озорства и «спортивного» азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются в психологическом плане как своеобразный вызов личности, их способностям.

К числу особенностей совершения преступления данной категории лиц можно отнести следующие:

1) отсутствие целеустремленной, продуманной подготовки к преступлению;

2) оригинальность способа совершения преступления;

3) использование в качестве орудий преступления бытовых технических средств и предметов;

4) непринятие мер к сокрытию преступления;

5) совершение озорных действий на месте происшествия.

Во *вторую группу* входят лица, страдающие новым видом психических заболеваний — информационными болезнями или компьютерными фобиями. Изучением этих болезней в настоящее время занимается новая, сравнительно молодая отрасль медицины — информационная медицина. По данным специальной комиссии Всемирной организации здравоохранения, негативные последствия для здоровья человека при его частой продолжительной работе с персональным компьютером очевидны и являются объективной реальностью.

Преступления в сфере высоких информационных технологий могут совершаться лицами, страдающими указанным видом заболеваний. Скорее всего, при наличии подобных фактов в процессе раскрытия и расследования компьютерного преступления необходимо обязательное назначение специальной судебно-психиатрической экспертизы на предмет установления вменяемости преступника в момент совершения им преступных деяний. Это в свою очередь должно повлиять на квалификацию деяний преступника в случае судебного разбирательства (преступление, совершенное в состоянии аффекта или лицом, страдающим психическим заболеванием, и т. д.).

Можно сделать вывод о том, что преступления, совершаемые преступниками данной группы, в основном связаны с физическим уничтожением либо повреждением средств компьютерной техники без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями.

Третью группу составляют профессиональные преступники, с ярко выраженными корыстными целями. Они характеризуются многократностью совершения преступлений с обязательным использованием действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми преступными навыками. Преступники этой группы обычно являются членами хорошо организованных, мобильных и технически оснащенных высококлассным оборудованием и специальной техникой (нередко оперативно-технического характера) преступных групп и сообществ. Это высококвалифицированные специалисты, имеющие высшее техническое образование. Именно эта группа преступников и представляет собой основную угрозу для общества, является кадровым ядром преступности в сфере высоких информационных технологий, как в качественном, так и в количественном плане.

По категориям доступа к средствам компьютерной техники их можно разделить на две подгруппы:

– внутренние пользователи (лица, которые имеют непосредственный доступ к необходимой информации);

– внешние пользователи (субъекты, которые обращаются к информационной системе или посреднику за получением необходимой им информации).

По мнению респондентов (специалистов), подавляющее число преступлений (87 %) совершается именно внутренними пользователями (обычно это рабочие и служащие фирм и компаний). Внешние пользователи — это лица, которые хорошо осведомлены о деятельности потерпевшей стороны. Круг внешних пользователей настолько широк, что не поддается никакой систематизации и классификации (ими может быть практически любой человек).

Раскрывая личность преступника, необходимо также во всех случаях при расследовании преступления выяснить мотив и цель. Это имеет важное значение не только для определения судом справедливого наказания за содеянное, но и способствует полному раскрытию преступления. Сведения о наиболее распространенных мотивах и целях совершения преступлений используются при выдвижении версий относительно субъекта и субъективной стороны преступления, а также при организации целенаправленного поиска преступника [114; 115].

Характерными мотивами и целями преступлений в сфере высоких информационных технологий являются:

– незаконное получение денег, ценных бумаг, кредита, материальных ценностей, товаров, услуг, привилегий, льгот, квот, недвижимости, топливно-сырьевых и энергетических ресурсов, стратегического сырья;

– уклонение от уплаты налогов, платежей, сборов и т. п.;

– легализация (отмывание) преступных доходов;

– подделка или изготовление поддельных документов, штампов, печатей, бланков, денежных билетов в корыстных целях;

– получение конфиденциальной информации в корыстных или политических целях;

– месть на почве личных неприязненных отношений с администрацией или сослуживцами по работе;

– дезорганизация валютной системы страны в корыстных или политических целях;

– дестабилизация обстановки в стране, территориально-административном образовании, населенном пункте (в политических целях);

– дезорганизация работы учреждения, предприятия или системы с целью вымогательства, устранения конкурента или в политических целях;

– стремление скрыть другое преступление;

– хулиганские побуждения и озорство;

– исследовательские цели;

– демонстрация личных интеллектуальных способностей или превосходства и многое другое.

Из всего количества можно выделить пять наиболее распространенных мотивов совершения преступлений:

1) корыстные соображения — 66 % (совершаются в основном преступниками третьей группы — этот показатель подтверждается данными В. П. Панова [116, с. 14]);

2) политические цели — 17 % (шпионаж, например; совершаются преступниками третьей группы);

3) исследовательский интерес — 7 % (студенты и профессиональные программисты первой группы);

4) хулиганские побуждения и озорство — 5 % (хакеры — первая группа);

5) месть — 5 % (преступники первой и второй групп).

Также в настоящее время можно выделить некоторые преступные цели, для достижения которых преступники использовали средства компьютерной техники. Наиболее типичными преступными целями являются: подделка счетов и платежных ведомостей; приписка сверхурочных часов работы; фальсификация платежных документов; хищение наличных и безналичных денежных средств; вторичное получение уже произведенных выплат; перечисление денежных средств на фиктивные счета; отмывание денег; легализация преступных доходов; совершение покупок с фиктивной оплатой; незаконные валютные операции; незаконное получение кредитов; манипуляции с недвижимостью; получение незаконных льгот и услуг; продажа конфиденциальной информации; хищение материальных ценностей, товаров и т. п.

При этом, как правило, 52 % преступлений связано с хищением денежных средств; 16 % — с разрушением и уничтожением средств компьютерной техники; 12 % — с подменой исходных данных; 10 % — с хищением информации и программ и 10 % — связано с хищением услуг (Приложение А).

Исследуя вопрос возрастной характеристики преступников в сфере высоких информационных технологий, хотелось бы отметить, что на первой международной конференции Интерпола по компьютерной преступности, где обсуждалась противоправная деятельность хакеров, они были условно разделены на три группы.

К *первой* относится молодежь в возрасте 11-15 лет, которые в основном совершают кражи через кредитные карточки и телефонные номера, «взламывая» коды и пароли больше из-за любознательности и самоутверждения.

Ко *второй* группе отнесены лица в возрасте 17-25 лет. В основном это студенты, которые в целях повышения своего «познавательного» уровня устанавливают тесные отношения с хакерами других стран, посредством электронных сетей обмениваясь информацией и похищая ее из различных банков данных.

Третья группа — лица в возрасте 30-45 лет, которые умышленно совершают компьютерные преступления с целью получения материальной выгоды, а также ради уничтожения или повреждения компьютерных сетей, — так называемый «тип вандала» [117].

Однако данная выборка, по нашему мнению, не является репрезентативной. Ведь статистика ведется по «установленным» правонарушениям. В то же время официальные власти большинства стран (в том числе и США, где подобные преступления расследуются с 1966 г.) вынуждены признавать, что выявление нарушителя почти в 90 % случаев невозможно. На наш взгляд, наиболее опасные компьютерные преступления совершают лица в возрасте 25-35 лет, имеющие инженерное образование и продолжительный опыт работы в области информационных технологий в сфере системного администрирования или программирования на языках низкого уровня, неправомерная деятельность которых практически никогда не бывает наказана. При этом хотелось бы пояснить, что в информатике языки программирования подразделяются на языки высокого и низкого уровней. Наибольшие возможности, в том числе и по созданию языков программирования высокого уровня, имеют языки программирования низкого уровня — программирование в машинных кодах (язык Ассемблер). При этом специалисты по программированию в машинных кодах составляют элиту программистов.

Основная же часть раскрытых компьютерных преступлений совершается специалистами невысокой квалификации, знаний которых не хватает для того, чтобы скрыть следы своего преступления.

Представляет интерес способ характеристики преступников, данный российскими исследователями [52, с. 28], где на основе проведенного анализа возраста, образования, мотивации совершения преступления, даны основные характеризующие признаки компьютерных преступников (таблица 2).

В целом следует отметить, что возраст преступников колеблется от 15 до 45 лет. Например, по данным некоторых исследователей [114, с. 270], на момент совершения преступления возраст у 33 % преступников не превышал 20 лет, 13 % — старше 40 лет и 54 % — 20-40 лет.

Таблица 2 — **Основные характеризующие признаки компьютерных преступников**

тип	Возраст	Образование	род деятельности	дополнительно
Начинающий	14-20	Среднее, среднее специальное, незаконченное высшее. Как правило, образование техническое.	Безработные, либо подрабатывающие т. н. «компьютерщиками» в небольших фирмах. Набор общетехнических знаний: несколько языков программирования, аппаратная часть.	Неуравновешенны, имеют проблемы с общением, фанатизм в отношении компьютерной техники. Информацию находят в сетях Internet, Fidonet, при встречах с единомышленниками. Используют клички (никнеймы, «ники» — от англ. nickname), причем нередко и при личном общении. Используют компьютерный жаргон, смешивают английский и русский языки, часто безграмотны, гуманитарными науками не интересуются. Преступная деятельность начинается рано, как правило, неосознанно. Мотивы: романтика, корысть, хулиганство, месть.
Любитель	16-25	Техническое, но возможно и гуманитарное высшее либо незаконченное высшее образование.	Работа по специальности, возможно программистом, техническим консультантом или системным администратором. Знания более систематизированы.	Имеют сформировавшуюся систему взглядов и ценностей. Используют готовые решения, как правило, имеют и собирают необходимую документацию и программы. Преступная ориентировка возникает либо в результате трансформации из начинающего, либо непосредственно путем резкого погружения в криминальную среду с помощью коллег, друзей и т. п. Особых отличий от обычных людей нет. Клички могут использоваться в целях сокрытия реального имени. Мотивы: корысть, месть, самоутверждение, исследовательский интерес.

Продолжение таблицы 2

тип	возраст	образование	род деятельности	дополнительно
Профессионал	22-45	Возможно, имеют несколько высших. Техническое, юридическое, экономическое.	Исчерпывающие знания, возможно, мультиплатформенные. Как правило, достаточно независимы от работодателя. Возможно, собственное дело.	Крайне устойчивая психика, иногда тип лидера. Самостоятельно формируют цели и пути их достижения. Привлекают новичков и любителей к выполнению монотонной работы. Общение на профессиональном уровне ограничено узким кругом людей и повышенной конфиденциальностью. Мотивация: корысть, политические, иногда «профессиональная гордость».

В заключение рассматриваемого вопроса хотелось бы отметить, что в ходе расследования преступлений в сфере высоких информационных технологий целесообразно применять прогнозирование индивидуального и преступного группового поведения. Полезную информацию может дать и анализ платежей клиентов за телефонные услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Именно прошлое их поведение (судимость, правонарушения, антиобщественные поступки, большие успехи в области программирования), а также настоящее (поддержание криминальных связей, склонность создавать программы «вандалы») дают основания для прогностических выводов о вероятном противоправном поведении в будущем. Принимаются во внимание социальные оценки, даваемые лицу, представляющему оперативный интерес, играет роль для него мнения представителей криминогенной и преступной среды. Все это в совокупности является элементами методики прогнозирования, в которую вплетаются следственно-оперативные мероприятия. Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные технологии.

В ряде составов преступлений в сфере высоких информационных технологий мотивация поведения преступника имеет особое значение. Преступные мотивы есть по сути своей модификации обычных человеческих мотивов, но направленные на цели, запрещенные законом или связанные с использованием противоправных средств. Поэтому для осуществления качества расследования и раскрытия преступлений определенный интерес представляют социологические и психологические исследования молодежи, обучающейся компьютерным наукам. Для профилактической деятельности по предотвращению преступлений в сфере высоких технологий важно проводить изучения мотивов поступков

человека. Особый интерес представляет определение уровня ценностно-ориентационного единства в молодежной аудитории. По данному уровню можно определить факторы, влияющие на поведение человека в группах и, в какой-то степени, спрогнозировать его стремления к противоправным действиям.

При выявлении и раскрытии преступлений в сфере высоких технологий сотрудник сталкивается с нетрадиционными следами преступной деятельности или вещественными доказательствами. Поэтому для грамотного использования фактических данных, полученных в ходе осуществления следственно-оперативных мероприятий по таким преступлениям, базовой юридической подготовки может оказаться недостаточно. Для успешного осуществления раскрытия преступлений в сфере высоких технологий сотрудникам необходимо хорошее знание психологии хакера, знать его тактику проведения атак на компьютерные системы, уровень его знаний и возможность их пополнения.

Также расследование преступления, несмотря на то, что каждый считается невиновным, пока его виновность в совершении преступления не будет доказана в предусмотренном Уголовно-процессуальным кодексом порядке [118], так или иначе, не может происходить отвлеченно от утверждений о виновности либо невиновности лица, доказывании отдельных обстоятельств отвечающих на этот вопрос. В этой связи, Уголовно-процессуальный кодекс играет важнейшую функцию определения порядка доказывания обстоятельств имеющих значение для решения вопроса о виновности либо невиновности лица других вопросов, имеющих значение и требующих доказывания. Эти вопросы определяются ст. 117 УПК РК «Обстоятельства подлежащие доказыванию по уголовному делу» и имеют следующий вид:

1. По уголовному делу подлежат доказыванию:

1) событие и предусмотренные уголовным законом признаки состава преступления (время, место, способ и другие обстоятельства совершения преступления);

2) кто совершил запрещенное уголовным законом деяние;

3) виновность лица, в совершении запрещенного уголовным законом деяния, форма его вины, мотивы совершенного деяния, юридическая и фактическая ошибки;

4) обстоятельства, влияющие на степень и характер ответственности обвиняемого;

5) обстоятельства, характеризующие личность обвиняемого;

6) последствия совершенного преступления;

7) характер и размер вреда причиненного преступлением;

8) обстоятельства, исключающие преступность деяния;

9) обстоятельства, влекущие освобождение от уголовной ответственности и наказания;

10) дополнительные обстоятельства, подлежащие доказыванию по делам о преступлениях совершенных несовершеннолетними, указанными в ст. 481 УПК РК «Обстоятельства, подлежащие установлению по делам о преступлениях несовершеннолетних»;

11) обстоятельства, способствовавшие совершению преступления.

Вместе с тем, очевидно, что перечисленные обстоятельства, имея характер нормы права, обладают всеми присущими для нормы права качествами. К примеру, носят характер общеобязательности, т. е. являются безличным, неперсонифицированным правилом поведения, которое распространяется на большое количество жизненных ситуаций и большой круг лиц [119, с. 273]. Между тем, такая безличность и неперсонифицированность, обладая положительными моментами, не может сама по себе определить конкретный, адресный круг обстоятельств, требующих установления в ходе расследования преступлений в сфере высоких технологий и любого другого преступления, в частности.

В этой связи следует обратить особое внимание на определение обстоятельств, подлежащих установлению по уголовному делу, которые определяются как «конкретно-определенные факты, отражающие сущность, механизм расследуемого преступления, а также прочие обстоятельства, подлежащие доказыванию по уголовному делу» [120, с. 50].

Здесь же следует обратить внимание на важность рассматриваемого вопроса с точки зрения расследования преступлений в сфере высоких информационных технологий, поскольку указанная категория деяний «находится на стыке права и технологии» [121, с. 81].

Обобщение практики расследования преступлений в сфере высоких информационных технологий позволяет выделить следующие основные обстоятельства, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории:

1. Наличие преступления (либо это правонарушение иного рода); непосредственная причина (причины) нарушения безопасности компьютерной информации и орудий ее обработки; не является ли происшедшее следствием непреодолимых факторов.

2. Объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности).

3. Предмет преступного посягательства.

4. Способ совершения преступления.

5. Наименование и назначение объекта, где совершено преступление.

6. Конкретное место совершения преступления в данном предприятии, учреждении, организации, на участке местности; наличие иных мест совершения преступления (было ли преступление совершено дистанционно вне помещения — по каналам электросвязи и локальной вычислительной сети).

7. Режим работы объекта.

8. Средства вычислительной техники и компьютерной информации, с помощью которых совершено преступление (тип, вид, модификация, функциональное назначение, техническое состояние и другие характеристики). Конкретный терминал или участок сети (абонентский номер, код, шифр, рабочая частота).

9. Режим работы СВТ.

10. Возможность утечки конфиденциальной информации.

11. Период (дата, время) совершения преступления.

12. Размер материального ущерба, из чего он складывается.

13. Служебные действия и операции технологического процесса, с которыми связано преступление; перечень должностных лиц или работников, несущих ответственность и имеющих непосредственное отношение к данным действиям (операциям) в силу технологии производства или командно-административного управления.

14. Мотив совершения преступления (корысть, месть, хулиганские побуждения, демонстрация личных интеллектуальных способностей, с целью сокрытия другого преступления и др.); цели, преследуемые и достигнутые преступником; наличие у преступника в момент совершения преступления состоянии внезапно возникшего сильного душевного волнения, аффекта, либо психического заболевания (информационного невроза или компьютерной фобии).

15. Субъект преступления, его характеристика. Если преступление совершено группой лиц, анализ ее состава и роли каждого соучастника.

16. Наличие причинной связи деяний с наступившими последствиями. Необходимо проверить и доказать, что именно деяния данного лица и обязательно те, которые ему инкриминируются, являются причиной наступивших последствий, например, наличие минимально необходимых специальных познаний у преступника.

17. Причины и условия, способствовавшие подготовке, совершению и сокрытию преступления; факторы, усугубившие их проявление (нарушения нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам; не подлежат ли они привлечению к уголовной ответственности за допущенные нарушения, способствовавшие совершению расследуемого преступления).

Подводя итог всему вышесказанному, можно сделать следующие выводы:

1. Криминалистическая характеристика преступлений в сфере высоких информационных технологий содержит систему обобщенных данных о типичных способах совершения преступления, орудиях и средствах, применяемых при совершении преступлений в сфере высоких технологий; обстановке, месте и времени совершения преступлений; о личности преступника, мотивах и целях его преступного поведения.

2. Способов совершения преступлений становится все больше и больше. Это происходит по мере совершенствования средств компьютерной техники. Хочется надеяться, что эта проблема будет глубже изучена отечественной криминалистикой, так как по проведенному исследованию о существовании тех или иных способов совершения компьютерных преступлений знают всего около 10 % респондентов.

3. Орудиями совершения преступлений в сфере высоких информационных технологий являются компьютер и технические средства, используемые непосредственно для незаконного получения сведений (радиопередающая и звукозаписывающая аппаратура, устройства прослушивания, встраиваемые в аппара-

туру обработки информации (т. н. «жучки», «таблетки», «клопы» и т. п.); спецмикрофоны с цифровыми адаптивными фильтрами типа АФ-512, DAC-256 и DAC-1024, позволяющие проводить обработку зашумленных речевых сигналов и т. п.).

4. Средствами совершения преступлений в сфере высоких информационных технологий являются: сетевое оборудование, телефонная сеть, телефон, телевизионный кабель, компьютерные системы, контрольно-измерительная аппаратура, устройства для регистрации электромагнитного излучения, специальное программное обеспечение, периферийное оборудование (принтер, CD-ROM — накопитель, стример, дисководы), а также носители компьютерной информации (дискеты, лазерные диски, флэш-карты) и т. д.

5. Местом, где в результате совершения рассматриваемого преступления наступил преступный результат, являются предприятия, организации, учреждения различных форм собственности, имеющие информацию на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети, т. е. преимущественно те, в которых используются высокие технологии.

6. Время совершения преступления зависит от способа его совершения и объекта, где расположена компьютерная техника. Так, при опосредованных и смешанных способах совершения преступления, связанных с использованием компьютерных сетей и, прежде всего, сети Интернет, преступники выбирают вечерние и ночные часы (с 20.00 до 6.00). Это объясняется тем, что в указанное время тарифы фирм-провайдеров по доступу в сеть ниже, чем днем, а также меньше нагрузка на сети, соответственно выше скорость обмена данными.

При способах совершения преступлений, связанных с непосредственным доступом к компьютерной информации, время определяется режимом работы объекта, где расположена компьютерная техника, то есть это рабочие часы с 9.00 до 18.00.

7. Субъект неправомерного доступа к компьютерной информации — лицо мужского пола (хотя количество женщин, совершающих компьютерные преступления, с каждым годом возрастает), высококлассный специалист-программист, профессионал с большим опытом работы, являющийся незаурядной, неординарной личностью, готов принять вызов, настроен на соперничество и противоборство, боится разоблачения, потери уважения, его поведение несколько отклоняется от принятых в обществе норм; он пользуется доверием по службе и имеет свободный доступ к компьютерным системам; как правило, приходит на работу первым, а уходит с нее последним, практически никогда не берет отпуск. Свои действия объясняет тем, что считает их не чем иным, как игрой. Все вышеперечисленное можно считать собирательным понятием «компьютерного преступника».

8. По категориям доступа к средствам компьютерной техники субъектов преступлений в сфере высоких информационных технологий можно разделить на две подгруппы:

– внутренние пользователи (лица, которые имеют непосредственный доступ к необходимой информации);

– внешние пользователи (субъекты, которые обращаются к информационной системе или посреднику за получением необходимой им информации).

9. Наиболее распространенными мотивами совершения преступлений в сфере высоких информационных технологий являются: 1) корыстные соображения — 66 %; 2) политические цели — 17 %; 3) исследовательский интерес — 7 %; 4) хулиганские побуждения и озорство — 5 %; 5) месть — 5 %.

Наиболее типичными преступными целями совершения преступлений в сфере высоких информационных технологий являются: 52 % — хищение денежных средств; 16 % — разрушение и уничтожение средств компьютерной техники; 12 % — подмена исходных данных; 10 % — хищение информации и программ и 10 % — хищение услуг.

10. Обстоятельства, подлежащие доказыванию и установлению по делу, — конкретно-определенные факты, отражающие сущность, механизм, расследуемого преступления, а также прочие обстоятельства, подлежащие доказыванию по уголовному делу. Обобщение практики расследования преступлений в сфере высоких информационных технологий позволяет выделить семнадцать основных обстоятельств, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории.

3 ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

3.1 Типичные исходные следственные ситуации, алгоритмизация первоначального этапа расследования преступлений в сфере высоких информационных технологий

Одна из особенностей преступлений в сфере высоких информационных технологий, как нами уже было отмечено, заключается в том, что они чрезвычайно латентны (около 90 %). Это связано с тем, что после совершения компьютерного преступления потерпевший обычно не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность (но это проявляется не во всех случаях). Возможные причины подобного поведения — жертва компьютерного преступления, как правило, совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты, например, банком своей репутации) существенно превосходят уже причиненный ущерб, а сам преступник в результате огласки приобретает широкую известность в деловых и криминальных кругах.

Между тем, раскрывать преступления, совершаемые в сфере высоких информационных технологий, сложно, т. к. нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место. К ним, как правило, относятся:

– естественные: стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т. п.); самопроизвольное разрушение элементов, составляющих СВТ;

– обусловленные неумышленной деятельностью человека вследствие непреодолимых факторов [52, с. 32]. Это ошибки в следующих случаях: при создании (изготовлении) СВТ (недочеты проектирования, в т. ч. системы защиты, кодирования информации, в изготовлении элементов СВТ); в процессе работы (эксплуатации) СВТ (неадекватность концепции обеспечения безопасности СВТ; недочеты управления системой защиты, ошибки персонала, сбои и отказы оборудования и программного обеспечения, ошибки при производстве пусконаладочных и ремонтных работ).

В криминалистической науке установлено, что определение основных направлений расследования и особенности тактики отдельных следственных действий зависят от характера исходных данных. В связи с этим в юридической литературе неоднократно предпринимались попытки систематизации исходных данных, в результате чего появилось понятие исходной следственной ситуации [74, с. 129-148; 122, с. 10-21; 123, с. 13; 124]. Под исходной следственной ситуацией понимается объективно сложившаяся в первый период расследования его информационная среда, обстановка проведения и другие условия расследования [122, с. 14], от которых зависит тактика и последовательность проведения

первоначальных следственных действий, оперативно-розыскных и организационных мероприятий. По делам рассматриваемой категории можно выделить следующие исходные следственные ситуации:

1. Информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируются и осуществляются следующие первоначальные следственные действия, оперативно-розыскные и организационные мероприятия:

– допрос заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей;

– решение вопроса о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

– вызов необходимых специалистов для участия в осмотре места происшествия;

– осмотр места происшествия;

– проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств;

– выемка и последующий осмотр средств электронно-вычислительной техники, предметов, материалов и документов (в т. ч. находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия;

– допросы свидетелей (очевидцев);

– допросы подозреваемых (свидетелей), ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации;

– обыски на рабочих местах и по месту проживания подозреваемых;

– назначение программно-технической, радиотехнической, технической, бухгалтерской и иных экспертиз;

– дальнейшие действия, которые планируются с учетом дополнительной информации.

Для третьей следственной ситуации может быть предложена следующая программа расследования и действий следователя на первоначальном этапе:

– изучение поступивших материалов с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка передачи в органы следствия. При необходимости принятие мер к получению недостающей информации;

– возбуждение уголовного дела;

– вызов необходимых специалистов для участия в осмотре места происшествия;

– осмотр места происшествия;

– личные обыски задержанных, их рабочих мест и места проживания;

– допрос подозреваемых;

– выемка и осмотр вещественных и письменных доказательств;

– изъятие и осмотр подлинных документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в т. ч. и тех документов, которые находятся в электронной форме на машинных носителях информации);

– допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за работу (денежные средства, материальные ценности, услуги и т. п.) по фактам установленных нарушений;

– истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении (в т. ч. с конфиденциальной информацией, бланками строгой отчетности, использование СВТ и т. п.);

– допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с лицами, совершившими преступные действия;

– анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведения ревизии или проверки, в т. ч. повторной (по каким позициям, за какой период и с участием каких специалистов).

При выполнении вышеуказанных программ следует учитывать особенности методики расследования конкретного вида преступления, о совершении которого выдвинуты версии. Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

1. Преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике.

2. Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3. Преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

4. Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

5. Преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов.

6. Ложное заявление о преступлении.

Приведенный перечень следственных версий является общим, и в зависимости от конкретной ситуации может быть расширен. При этом типичными частными версиями являются версии:

– о личности преступника (преступников);

– о способах совершения преступления;

– об обстоятельствах, при которых было совершено преступление;

– о размерах ущерба, причиненного преступлением.

Как нами было указано выше ст. 227 УК РК фактически предусматривает ответственность за совершение трех составов преступлений: неправомерный доступ к охраняемой законом компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Рассмотрим особенности расследования данных преступлений более подробно. Данную необходимость обуславливает дефицит криминалистических рекомендаций по методике и тактике расследования указанных составов преступлений, в связи с чем, представляется обоснованным предложить методические рекомендации и схемы расследования указанных преступлений, которые будет выглядеть следующим образом.

1. **Первоначальный этап расследования неправомерного доступа к охраняемой законом компьютерной информации.**

Признаками совершения указанного состава могут являться:

– появление в компьютере фальшивых или искаженных данных;

– необновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

– частые сбои в процессе работы компьютеров;

– участившиеся жалобы клиентов компьютерной системы или сети;

– осуществление сверхурочных работ без видимых на то причин;

– немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;

– неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;

– чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительными предлогами;

– участившиеся случаи перезаписи отдельных данных без серьезных на то причин;

– чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

При наличии указанных признаков либо иного сигнала о совершенном преступлении следует установить [85, с. 49]:

1. Факт неправомерного доступа к компьютерной информации.

2. Место несанкционированного проникновения в компьютерную систему или сеть.

3. Время несанкционированного доступа.

4. Надежность средств защиты компьютерной информации.

5. Способ совершения несанкционированного доступа.

6. Круг лиц, совершивших неправомерный доступ

7. Виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации.

8. Наличие последствий преступления.

9. Наличие обстоятельств, способствовавших преступлению.

Факт неправомерного доступа к информации в компьютерной системе или сети обычно первыми обнаруживают сами же пользователи информационной системы. Однако они не всегда своевременно сообщают об этом правоохранительным органам. Особенно это относится к руководителям кредитно-финансовых и банковских учреждений, которые не желают вызывать у клиентов сомнения в надежности своих учреждений. Они также опасаются, что по этому факту начнется проведение проверок, ревизий и экспертиз, могущих раскрыть их финансовые и иные служебные тайны, вскрыть другие серьезные недостатки.

Факт несанкционированного доступа в сети Интернет вскрывается уже после того, как фирма-провайдер присылает счет о предоставленных услугах на сумму, явно превышающую допустимые пределы работы зарегистрированного пользователя. Кроме того, время работы также не соответствует действительности. В результате этого официально зарегистрированный пользователь отказывается платить за услуги, которыми не пользовался, а фирма-провайдер соответственно несет убытки. Возможны и другие варианты развития событий. Например, в случае если официально зарегистрированный пользователь превышает данные ему полномочия и вносит изменения в страницы, принадлежащие другим пользователям.

Установить факт неправомерного доступа к компьютерной информации можно и в процессе проведения проверочных мероприятий в стадии возбуждения уголовного дела либо в ходе проведения ревизий, судебных экспертиз, иных следственных действий по уголовным делам, находящимся в производстве следователей, а также при проведении оперативно-розыскных мероприятий.

Установление *места несанкционированного доступа в компьютерную систему или сеть* может вызывать определенные трудности, поскольку по делам данной категории может быть несколько мест совершения одного преступления.

Чаще обнаруживается место неправомерного доступа к компьютерной информации по преступлениям, связанным с хищением денежных средств. Так, по делу о покушении на хищение из Центрального банка РФ более 68 миллиардов рублей таких мест оказалось сразу девять: одно из них — само помещение этого банка, и восемь — помещения коммерческих банков, в адрес которых были незаконно переведены из Центрального банка по компьютерной сети крупные суммы денег путем ввода в электронную обработку двенадцати фальшивых платежных документов. Как выяснилось позже, вводились они неуста-

новленными лицами с рабочего места № 83 оператором ввода № 07 с терминала № 07 [125, с. 348].

На всех этих местах должны были остаться следы одного преступления. Однако на первоначальном этапе расследования установить физический адрес ввода фальшивых документов так и не удалось. По мнению специалистов, в той ситуации такой ввод мог быть осуществлен с любого рабочего места, имеющего телекоммуникационную связь с компьютерами. Тем более что эксплуатируемый программный комплекс фактически был открыт для несанкционированного ввода, обновления (корректировки, изменения) и обработки любой информации. Поэтому при обнаружении неправомерного доступа к информации в компьютерной системе или сети следует выявить все места, где расположены компьютеры, имеющие единую телекоммуникационную связь.

Проще обстоит дело, когда совершен несанкционированный доступ к отдельному изолированному компьютеру, находящемуся в одном помещении. Однако и в этом случае необходимо учитывать, что компьютер может находиться в одном помещении, а информация на машинных носителях — в другом. Следовательно, надо выявить и это место.

Труднее устанавливать место непосредственного использования технических средств для несанкционированного доступа (особенно мобильных), не входящих в данную компьютерную систему или сеть. В данном случае следует установить и место хранения информации на машинных носителях либо в виде распечаток, добытых в результате неправомерного доступа к компьютерной системе или сети.

Установление времени несанкционированного доступа. Любой современный компьютер имеет встроенный таймер, отражающий информацию о дне недели, дате, часе и минуте в реальном времени. Естественно, что его точность определяется правильностью первоначальной установки времени, выбором правильного часового пояса, а также переходом на летнее или зимнее время. Время последней модификации файла отражается в его атрибутах и достаточно просто может быть выяснено с помощью программ общесистемного назначения.

Кроме того, при входе в систему или сеть время работы на компьютере любого пользователя автоматически фиксируется в специальных системных файлах. Исходя из этого, точное время доступа можно установить путем следственного осмотра работающего компьютера либо распечаток или дискет. Время неправомерного доступа к компьютерной информации можно также установить путем допроса свидетелей из числа сотрудников данной компьютерной системы, выясняя у них, в какое время каждый из них работал на компьютере, если оно не было зафиксировано автоматически.

Установление способа совершения несанкционированного доступа. Конкретный способ несанкционированного доступа к компьютерной информации можно установить в процессе допроса свидетелей из числа лиц, обслуживающих эту систему, или ее разработчиков, а также путем производства судебно-технологической экспертизы.

Для установления способа и отдельных обстоятельств механизма неправомерного доступа к компьютерной информации может быть проведен следственный эксперимент с целью проверки возможности преодоления средств защиты компьютерной системы одним из вероятных способов.

При установлении надежности средств защиты компьютерной информации необходимо, прежде всего, установить, предусмотрены ли вообще в данной компьютерной системе меры защиты от несанкционированного доступа к определенным файлам. Это можно выяснить при допросе разработчиков и пользователей, а также при изучении проектной документации и соответствующих инструкций по эксплуатации данной системы. В них должны содержаться специальные разделы, относящиеся к мерам защиты информации, с подробным описанием порядка допуска пользователей к определенным категориям данных (т. е. разграничением их полномочий), организации за доступом контроля, конкретных методов защиты информации (аппаратных, программных, криптографических, организационных и пр.).

Законодательством предусмотрены обязательная сертификация средств защиты систем обработки и хранения информации с ограниченным доступом, обязательное лицензирование всех видов деятельности в области проектирования и производства таких средств. Разработчики, как правило, гарантируют надежность своих средств при условии соблюдения установленных требований. Поэтому в процессе расследования требуется установить: во-первых, имеется ли лицензия на производство средств защиты информации от несанкционированного доступа, используемых в данной компьютерной системе; во-вторых, соответствуют ли их параметры выданному сертификату. Для проверки такого соответствия назначается судебно-технологическая экспертиза.

При исследовании объекта, где совершено преступление, необходимо выяснить:

– технические и конструктивные особенности помещений, связанные с установкой и эксплуатацией вычислительной техники (специальное оборудование полов, потолков и окон, каналы кабельных и вентиляционных шахт, установка и фактическое состояние устройств кондиционирования воздуха, система электропитания и иные особенности);

– особенности установки средств комплекса вычислительной техники (сосредоточены в одном месте или расположены в различных помещениях);

– способы связи компьютеров между собой посредством локально-вычислительной сети, устройств телекоммуникации и состояние линий связи;

– структуру, конфигурацию сети ЭВМ и внешних информационных связей;

– режим работы.

Установление лиц, совершивших неправомерный доступ к компьютерной информации. Опрос респондентов из числа лиц, обладающих специальными знаниями в сфере высоких технологий, показывает, что чем хитрее и сложнее в техническом плане способ такого проникновения, тем легче «вычислить» пре-

ступника, поскольку круг специалистов, обладающих такими способностями, сужается.

Причастность конкретного лица к несанкционированному доступу к компьютерной информации помимо свидетельских показаний может быть установлена также и по материально-фиксированным отображениям, обнаруженным при производстве следственного осмотра компьютера и его компонентов. Это могут быть следы пальцев рук, оставленные на их поверхности, отдельные записи на внешней упаковке дискет, дисков, где обычно остаются заметки о характере записанной на них информации, а порой и о том, кому принадлежат эти носители информации; следы обуви и другие материальные следы. Для их исследования назначаются традиционные криминалистические экспертизы, дактилоскопические, почерковедческие, трасологические, а также техническое исследование документов.

Чтобы выявить лиц, обязанных обеспечивать соблюдение режима доступа к компьютерной системе или сети, необходимо, прежде всего, ознакомиться с имеющимися инструкциями, устанавливающими полномочия должностных лиц, ответственных за защиту информации, после чего следует их допросить. При допросе лиц, обслуживающих компьютерную систему, можно установить: кто запускал нештатную программу, было ли это зафиксировано каким-либо способом? Следует также выяснить, кто увлекался программированием (возможно, кто-то учится или учился на компьютерных курсах).

При наличии достаточных оснований у лиц, подозреваемых в неправомерном доступе к компьютерной информации, производится обыск, в процессе которого могут быть обнаружены компьютерная техника, различные записи, дискеты, содержащие сведения, могущие иметь отношение к расследуемому событию, например коды, пароли, идентификационные номера пользователей конкретной компьютерной системы, а также данные о ее пользователях.

Установление виновности и мотивов лиц, совершивших неправомерный доступ к компьютерной информации можно только по совокупности результатов всех процессуальных действий. Решающими из них являются допросы свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, результаты обыска.

При установлении последствий неправомерного доступа к компьютерным системам или сетям необходимо, прежде всего, выявить — в чем выражены вредные последствия такого доступа (хищение денежных средств или материальных ценностей, завладение компьютерными программами, информацией путем изъятия ее машинных носителей либо копирования, а также незаконное изменение, уничтожение, блокирование или вывод из строя компьютерного оборудования, введение в компьютерную систему заведомо ложной информации или компьютерного вируса и пр.). Хищение денежных средств в банковских электронных системах зачастую обнаруживаются самими работниками банков или в результате проведения оперативно-розыскных мероприятий. Конкретная сумма хищения устанавливается судебно-бухгалтерской экспертизой.

При выявлении обстоятельств, способствовавших неправомерному доступу к компьютерной информации, формируется целостное представление о данных обстоятельствах. С этой целью изучаются документы, относящиеся к защите информации, и заключение технологической экспертизы. Если по факту неправомерного доступа проводилось внутреннее (служебное) расследование, то его выводы также могут оказаться полезными при выявлении причин и условий его совершения.

2. **Первоначальный этап расследования создания, использования и распространения вредоносных программ для ЭВМ.**

Признаков совершения данных преступлений нет. Как правило, обнаружить можно лишь их результаты — сбои в процессе работы компьютерной системы или сети, жалобы клиентов и т. п.

При расследовании создания вредоносных программ для ЭВМ подлежат установлению следующие обстоятельства [126]:

– факт создания вредоносной программы для ЭВМ;

– способ создания вредоносной программы;

– факт использования и распространения вирусной программы.

– предназначение вредоносной программы и механизм действия;

– место, время создания, используемое для этого программное обеспечение и компьютерная техника;

– круг лиц, виновных в создании, использовании и распространении вирусных программ для ЭВМ.

– цель и мотив создания программы;

– осведомленность лица, использовавшего программу, о ее вредоносных свойствах, наличие или отсутствие умысла на использование и распространение данной программы;

– характер и размер вреда, причиненного данным преступлением;

– наличие обстоятельств, способствовавших совершению расследуемого преступления.

Вредоносная программа, как правило, обнаруживается в момент, когда уже явно проявляются последствия ее применения. Вместе с тем она может быть обнаружена и на машинных носителях информации, в частности, путем изучения информации обложки компакт-диска. Кроме того, выявляется она также в процессе антивирусной проверки, производимой пользователем компьютерной системы перед началом работы на компьютере, особенно часто практикуемой при использовании чужих машинных носителей или получении электронной почты. Примером создания вредоносной программы без ее использования может служить следующее дело. Так, гр-н С. в период августа-сентября 2001 г. с использованием средства разработки «Delphi» создал вредоносную программу «Win$py», которая работает в среде «ОС Windows 95/98», предназначенную для перехвата паролей пользователя (без ведома последнего). Перехваченные пароли автоматически отправляются (копируются) указанной программой через компьютерную сеть Интернета на адрес электронной почты автора программы

либо любого другого лица, чей электронный адрес он указал. Затем он разместил рекламу данной программы в сети Интернет, в результате чего был задержан с поличным при попытке реализовать дискету с названной программой за 200 долларов США [127].

Основные направления использования вредоносных программ для ЭВМ рассмотрим на следующем примере: С., работая программистом предприятия электрических и тепловых сетей, имея доступ к компьютеру «Пентиум-1» абонентского отдела, с корыстной целью, 24 февраля 2002 г. умышленно внес изменения в существующую на предприятии компьютерную программу путем замены функций, выполняющихся при выборе пунктов меню программы. При попытке выполнения определенных пунктов меню на экране компьютера появлялась рамка с надписью, что по вопросам эксплуатации программы надо обращаться к С., что привело к несанкционированному блокированию компьютерной программы, нарушена работа ЭВМ, предприятию электросетей причинен материальный ущерб на сумму 210 тысячи тенге [128]. При этом расследование осуществлялось по следующим направлениям:

– получение заявления директора предприятия теплосетей с просьбой привлечь к уголовной ответственности С. за блокирование программы компьютера;

– проведение осмотра места происшествия, из которого усматривается, что в абонентском отделе предприятия теплосетей не может быть запущена программа;

– осуществление выемки системного блока компьютера «Пентиум-1» и руководства по пользованию программой;

– проведение осмотра системного блока компьютера «Пентиум-1», из которого усматривается, что на его жестком диске находится данная программа;

– установление и допрос свидетелей, показавших, что им известно о выходе из строя компьютера в абонентском отделе и невозможности работы с программой;

– назначение программно-технической экспертизы, из заключения которой усматривается, что функциональность программы нарушена в результате замены функций, выполняющих действия при выборе пунктов меню и это связано с умышленным внесением в программу изменений. Восстановление функциональности программы невозможно, поскольку отсутствуют необходимые для ее восстановления материалы и документация;

– проведение допроса представителя гражданского истца, показавшего назначение программы и размер ущерба в результате ее блокирования;

– проведение допроса обвиняемого, в котором он признал себя частично виновным.

Особенности расследования распространения вредоносных программ рассмотрим на следующем примере. В сентябре 2000 г. Б., устроившись продавцом компьютерных компакт-дисков в торговый павильон Выставочного центра «Атакент» (г. Алматы), продал компьютерный компакт-диск «Хакер-2000», содержащий программы для ЭВМ, заведомо приводящие к несанкционированно-

му уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети [129].

Основными доказательствами, полученными в ходе расследования данного дела, являлись:

– рапорт оперативного уполномоченного, из которого следует, что в ходе контрольной закупки гражданин М. за 300 тенге приобрел у гражданина Б. компьютерный диск «Хакер-2000», на котором, как пояснил Б., находятся программы, предназначенные для взлома компьютерных сетей и бесплатного пользования сетью Интернет с использованием чужих реквизитов и паролей;

– акт контрольной закупки, в котором зафиксирован факт изъятия у Б. компьютерных компакт-дисков «Хакер-2000»;

– протокол допроса свидетеля М., показавшего, что он был приглашен сотрудниками в качестве покупателя для проведения контрольной закупки вредоносных программ для ЭВМ, для чего он обратился к продавцу торгового павильона, расположенного перед Выставочным центром «Атакент» (г. Алматы), оказавшемуся впоследствии Б., с просьбой показать ему компакт-диск «Хакер-2000» и пояснить, что он дает, на что Б. ответил, что программы на данном диске дают возможность бесплатного пользования сетью Интернет, а также на нем имеются программы-взломщики, после чего М. приобрел данный диск за 300 тенге;

– протоколы допросов свидетелей А. и В., показавших, что они были приглашены в качестве присутствующих при проведении контрольной закупки компьютерных компакт-дисков, содержащих вредоносные программы для ЭВМ, после объявления которой в ходе осмотра торгового павильона перед Выставочным центром «Атакент» (г. Алматы) были обнаружены еще 6 компакт-дисков «Шпионские штучки часть 2» и два компакт-диска «Хакер-2000», которые были изъяты, упакованы в полиэтиленовые пакеты, прошитые белой нитью, концы которой скреплены печатью МВД РК и подписаны участниками контрольной закупки;

– протокол осмотра вещественных доказательств — дисков, изъятых у Б. в ходе контрольной закупки;

– заключение программно-технической экспертизы, из выводов которой следует, что представленные эксперту диски являются машинными носителями для ЭВМ и некоторые из содержащихся в предоставленных на экспертизу дисков программ вредоносны для ЭВМ;

– протокол допроса эксперта, показавшего, что вредоносными являются все программы, находящиеся на диске «Хакер-2000» и «Шпионские штучки часть 2»;

– протокол допроса обвиняемого Б., в котором он признал свою вину.

Наибольшую сложность для расследования представляет совершение преступления в условиях неочевидности. Здесь основными направлениями расследования должны быть:

1) пресечение противоправной деятельности;

2) выяснение механизма преступления и уточнение отдельных его обстоятельств;

3) установление лица, распространяющего вредоносную программу;

4) получение сведений о личности потерпевших;

5) установление суммы материального ущерба;

6) сбор доказательств о причастности установленного лица к каждым выявленным эпизодам преступной деятельности;

7) выяснение причин и условий, способствовавших совершению преступления;

8) получение характеризующего личность обвиняемого материала.

Изучение следственной практики показало, что наиболее распространенными условиями, способствовавшими совершению данного преступления, являются: использование не сертифицированного программного обеспечения; использование нелегальных копий программ для ЭВМ; отсутствие резервных копий программ и системных файлов; отсутствие учета и контроля за доступом к компьютерным системам; использование компьютеров не по назначению (для компьютерных игр, обучения посторонних, написания программ лицами, в обязанности которых это не входит); нерегулярное проведение антивирусной проверки компьютерной системы и машинных носителей, и др.

Примером удачного расследования уголовного дела названной категории может служить уголовное дело [130], заведенное в мае 2005 г. Так, Б. заключил договор абонентского обслуживания с предприятием, осуществляющем предоставление услуг по доступу к информационной сети Интернет (провайдером), согласно которому Б. был предоставлен доступ в сеть Интернет, электронный почтовый ящик и возможность открыть персональную страницу на сервере провайдера. В апреле 2005 г. Б. с одного из серверов сети Интернет переписал на жесткий диск своего персонального компьютера программу «scfg.exe», которая позволяла создать и настроить вредоносную программу типа «троянский конь» на адрес электронного почтового ящика Б. При переносе и запуске данной программы другими пользователями сети Интернет она производила незаметную для пользователя незаконную пересылку электронного сообщения на адрес электронного почтового ящика Б., содержащего в себе регистрационные данные (имя, пароль, телефонный номер) данного пользователя сети Интернет. Указанную программу Б. поместил на свою персональную страницу, в результате чего она стала доступной для неограниченного числа пользователей. В пояснении к этой программе на своей персональной странице для маскировки своих преступных намерений Б. указал: «Данная программа выявляет в реестре наличие всяких “лажовых” ссылок и “багов”» — хотя на самом деле эта программа таких действий не производила и не могла произвести.

Таким образом, Б. создал программу-«агента», позволявшую ему получать регистрационные данные законных пользователей, используя которые у него появилась возможность входить в сеть Интернет под чужим именем и за чужой счет. Те пользователи, которые, получив доступ к персональной странице Б.,

переписывали и запускали созданную им программу, не желая того сообщали ему свои регистрационные данные.

Расследование данного дела осуществлялось следующим образом.

– получение заявления и проведение допроса директора фирмы-провайдера о обнаружении на персональной странице Б. вредоносной программы типа «троянский конь», с помощью которой выявлен несанкционированный доступ к компьютерной информации других пользователей сети Интернет, после чего Б. был закрыт доступ к своему электронному почтовому ящику и персональной странице;

– проведение допроса ведущего специалиста фирмы-провайдера, показавшего, что на имя сетевого администратора в электронный почтовый ящик поступило сообщение от одного из пользователей сети Интернет о том, что на странице с адресом «WWW.Users/ru:8081/», оказавшейся в последствии персональной страницей Б., находится файл типа «троянский конь». Проверкой антивирусной программой установлено, что данный файл заражен вредоносной программой «Trojan.PSW.Stealth.c», а его запуск приводит к несанкционированному пользователем отправлению электронного почтового сообщения в адрес электронного почтового ящика Б., содержащего регистрационные данные пользователей сети Интернет;

– выемка журнала регистрации работы абонента Б. (распечаткой лог-файла, ведущегося на сервере фирмы-провайдера), из которого видно, что 30 апреля в 7 часов 27 мин. Б. переписал на свою персональную страницу файл, как выяснилось, впоследствии зараженный вредоносной программой;

– проведение осмотра и выемки почтово-телеграфной корреспонденции, содержащейся в электронном почтовом ящике Б., в ходе которой установлено, что в нем находится 11 сообщений, поступивших с 30 апреля по 1 мая 2005 г.;

– назначение и получение заключения программно-технической экспертизы, согласно которому 4 почтовых сообщения содержат в себе регистрационные данные для подключения к сети Интернет. Получение данных сообщений является результатом запуска программ, установленных на компьютере пользователя, настроенных на отправление регистрационных данных в адрес электронного почтового ящика Б.;

– проведение обыска по месту жительства Б., в ходе которого изъяты системный блок персонального компьютера и 13 накопителей на гибких магнитных дисках (дискетах);

– проведение осмотра изъятых в ходе обыска по месту жительства Б. дискет, в ходе которого они были проверены на наличие на них вредоносных программ, и на одной из них было установлено наличие вредоносной программы «Trojan.PSWStelth.a»;

– назначение программно-технической экспертизы, подтвердившей, что программный код, идентифицируемый антивирусной программой как «Trojan.PSWStelth.c» содержится на дискете, изъятой в ходе обыска по месту жительства Б. в файле «SCFG.exe». Данный файл является исполняемым про-

граммными продуктом и предназначен для создания и настройки вредоносной программы типа «троянский конь». В качестве параметров настройки используются адрес электронной почты, псевдоним и будущее имя троянской программы;

– назначение программно-технической экспертизы, в ходе которой установлено, что на компьютере Б. имеются все необходимые программные средства для доступа в информационную сеть Интернет;

– осуществление выемки программного обеспечения, содержащегося на персональной странице Б. на сервере фирмы провайдера, в ходе которой с персональной странице Б. был изъят файл, в котором в ходе антивирусной проверки обнаружена программа «Trojan.PSWStelth.c»;

– назначение программно-технической экспертизы, установившей, что файл, изъятый с персональной страницы Б., является вредоносной программой, настроенной на несанкционированную передачу регистрационных данных о пользователе данного компьютера на электронный почтовый ящик Б., уведомление пользователей о вредоносном действии программы при ее функционировании не производится. Кроме того, экспертами сделан вывод, что содержимое файла, находящегося на обнаруженной в ходе обыска по месту жительства Б. дискете, идентично содержимому файла, получающегося при выполнении программы «scfg.exe», находящейся на той же дискете;

– проведение следственного эксперимента, в ходе которого были подтверждены следующие факты: наличия на персональной странице Б. файла — «троянского коня», возможности получения другими пользователями сети Интернет доступа к персональной странице Б. и копирования файлов, содержащихся на ней.

По совокупности доказательств Б. было предъявлено обвинение.

3. **Первоначальный этап расследования нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.**

При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети подлежат установлению следующие обстоятельства [126, с. 377]:

1) факт преступного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети;

2) место и время совершения преступления;

3) характер информации, являющейся предметом посягательства;

4) способ и механизм нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети;

5) характер и размер ущерба, причиненного преступлением;

6) виновность лица;

7) обстоятельства, способствовавшие совершению преступления.

В расследовании данной категории преступлений одной из главных проблем становится установление самого факта нарушения правил эксплуатации ЭВМ. Здесь необходимо, прежде всего, установить факт существования конкретных правил эксплуатации ЭВМ на данном объекте, к которым может относиться: техническая документация на приобретаемые компьютеры; конкретные

принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка; требования по сертификации компьютерных сетей и оборудования; должностные инструкции конкретных сотрудников; правила пользования компьютерными сетями [75, с. 45].

Факт нарушения правил эксплуатации ЭВМ обычно становится известным в первую очередь непосредственным владельцам и пользователям компьютерной системы или сети после обнаружения ими отсутствия необходимой информации или существенного изменения ее, когда это уже отрицательно отразилось на основной деятельности предприятия, организации, учреждения.

Для установления конкретного правила эксплуатации ЭВМ, нарушение которого привело к вредным последствиям, следователю целесообразно допросить всех лиц, работавших на ЭВМ или обслуживающих компьютерное оборудование в тот период, когда это произошло (с участием специалиста). При допросе необходимо выяснить: функциональные обязанности конкретного сотрудника при работе с ЭВМ (либо оборудованием к ней), какими правилами они установлены, имеет ли данное лицо доступ к ЭВМ, их системе или сети; какую конкретно работу на ЭВМ и в каком порядке данный сотрудник выполнял; когда произошел факт уничтожения, блокирования, модификации компьютерной информации или наступили иные вредные последствия; какие неполадки в компьютерной системе были обнаружены при работе на ЭВМ, не было ли при этом каких-то сбоев, которые могли бы причинить существенный вред компьютерной информации; какой установленный порядок при работе с компьютером мог быть нарушен в данной ситуации либо они явились следствием непредвиденных обстоятельств, если да, то с какими конкретно.

Факт нарушения правил эксплуатации ЭВМ может быть установлен по материалам служебного расследования. Поступившие следователю для решения вопроса о возбуждении уголовного дела материалы подлежат тщательному и всестороннему изучению. Следователь должен усмотреть в них основание для возбуждения уголовного дела — наличие достаточных данных, указывающих на признаки преступления.

Конкретное место нарушения правил эксплуатации ЭВМ устанавливается при осмотре рабочих мест пользователей ЭВМ, компьютерной системы или сети. Осмотру подлежат все компьютеры, подключенные к сети ЭВМ. Цель — установить местонахождение компьютера, эксплуатация которого привела к вредным последствиям в результате преступного нарушения определенных правил его использования.

Необходимо различать место нарушения и место наступления вредоносных последствий. Они не всегда совпадают, особенно если идет речь о нарушении правил эксплуатации компьютерных сетей, которые, как известно, представляют собой объединение отдельных персональных компьютеров, расположенных на расстоянии друг от друга, и предназначены для совместного использования информации и обращении к периферийному оборудованию (принтерам, прокси-серверам, и пр.). Осмотру подлежат: рабочие станции локальных вычисли-

тельных сетей, в качестве которых применяются персональные компьютеры, объединенные внутри здания или в пределах небольшой территории; файловый сервер, обслуживающий все рабочие станции и осуществляющий совместное использование файлов, размещаемых на его дисках; принтеры, которые тоже могут находиться далеко от того места, где расположена рабочая станция.

Таким образом, основная задача осмотров рабочих мест — установить, где расположена рабочая станция, эксплуатация которой осуществлялась с грубым нарушением правил информационной безопасности. В первую очередь необходимо обратить внимание на рабочие станции, имеющие собственные дисководы. У них значительно больше возможностей для преступных нарушений. Они, к примеру, имеют возможность копировать данные с файлового сервера на свою дискету или использовать дискеты с различными программами, в т. ч. с компьютерными вирусами, и подвергать опасности целостность информации, содержащейся в центральных файловых серверах, чего не имеют бездисковые рабочие станции. Таков один из важных признаков, по которому можно установить место совершения преступления.

Другой способ — это следственный осмотр учетных данных, где могут быть отражены сведения о расположении конкретной рабочей станции, использующей файловый сервер. Кроме того, с особой тщательностью подлежат осмотру рабочие места, имеющие собственные каналы выхода во внешние сети, в частности, в Интернет. При осмотре изучаются файлы истории, содержащие данные о последних посещениях различных сайтов, протоколы соединения, содержащие данные о имени и пароле пользователя, времени и продолжительности соединения.

При определении времени нарушения правил эксплуатации ЭВМ необходимо установить и зафиксировать раздельно: а) время нарушения конкретных правил; б) время наступления вредных последствий. Нарушение правил и наступление вредных последствий может произойти одновременно. И может быть значительный разрыв во времени между моментом нарушения правил и временем наступления вредных последствий. Так, к примеру, сначала вносятся изменения в программу или базу данных в нарушение установленных правил и в результате только через определенное время наступают вредные последствия, которые либо сразу обнаруживаются, либо через какое-то время.

Время нарушения правил обычно устанавливается по учетным данным, которые фиксируются в процессе эксплуатации ЭВМ. Такими данными могут быть: сведения, полученные в результате использования средств автоматического контроля компьютерной системы, ее регистрирующих пользователей, моменты подключения к ней абонентов, а также файлы учета сбойных ситуаций, книги (либо журналы) учета передачи смен операторами ЭВМ, распечатки выходной информации, где, как правило, фиксируется время ее обработки. Такие данные могут быть получены в результате проведения осмотра места происшествия, а также и выемки и осмотра необходимых документов.

В процессе осмотра места происшествия могут быть обнаружены машинные носители информации, на которых ранее хранились важные данные, а

вследствие нарушения определенных правил эксплуатации ЭВМ они оказались уничтоженными или существенно изменены либо допуск к ним стал невозможным (нужная информация оказалась заблокированной). На них может быть зафиксировано время наступления таких последствий.

Поскольку непосредственным предметом преступного посягательства является охраняемая законом информация ЭВМ, при расследовании рассматриваемой категории преступлений необходимо установить ее характер. Законом, как известно, охраняется любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении: а) сведений, отнесенных к государственной тайне; б) конфиденциальной информации; в) персональных данных. Поэтому в первую очередь требуется определить к какому из этих видов относится информация, которая была подвергнута уничтожению в результате преступного нарушения правил эксплуатации ЭВМ. Это устанавливается специальными органами, согласно соответствующим нормативным правовым актам (законодательством о государственной тайне, коммерческой тайне и персональных данных). Далее необходимо установить — кто является собственником или владельцем данных информационных ресурсов или информационной системы в целом, какова их стоимость.

Способ нарушения правил эксплуатации ЭВМ может быть активным или пассивным. Первый выражается в самовольном выполнении непредусмотренных операций при компьютерной обработке информации. Второй — в невыполнении предписанных действий.

Способ и механизм нарушения этих правил устанавливаются путем допросов свидетелей, подозреваемых и обвиняемых (желательно с участием специалистов), проведения следственного эксперимента или производства компьютерно-технической экспертизы. При допросах выясняется последовательность той или иной операции на ЭВМ, которая привела к нарушению правил. При проведении следственного эксперимента выясняется возможность наступления вредных последствий при нарушении определенных правил. Он проводится на копиях исследуемой информации и по возможности на той же ЭВМ, на которой произошло нарушение правил. Характер ущерба, наносимого преступным нарушением правил эксплуатации ЭВМ может заключаться в уничтожении, блокировании или модификации охраняемой законом информации.

Ущерб может носить экономический характер, когда охраняемая законом информация ЭВМ выступает как собственность, ценность которой определяется в денежном выражении; общегосударственный характер — когда в ней содержатся сведения, составляющие государственную тайну. Конкретный размер ущерба устанавливается допросом собственника информационных ресурсов, протоколами выемки и осмотра платежных документов, экономической экспертизой, перед которой может быть поставлен вопрос: «Какова стоимость информации, уничтоженной (или измененной) вследствие нарушения правил эксплуатации ЭВМ?».

При установлении лица, допустившего преступное нарушение правил эксплуатации ЭВМ, необходимо различать лицо, имеющее доступ к ЭВМ, а также лицо, имеющее право доступа к компьютерной информации. Не обязательно, чтобы лицо, имеющее доступ к ЭВМ, имело право на доступ к компьютерной информации, находящейся в ЭВМ. Доступ к ЭВМ, к системе ЭВМ или к сети, как правило, имеют лица в силу выполняемой ими работы, связанной с эксплуатацией или обслуживанием.

Все это устанавливается по результатам допросов свидетелей, обвиняемого, осмотра эксплуатационных документов по данной компьютерной системе, осмотра вещественных доказательств (компьютера, оборудования к нему, машинных носителей информации, распечаток и пр.).

Виновность лица, совершившего преступное нарушение правил эксплуатации ЭВМ, устанавливается на основе анализа результатов всех проведенных в ходе расследования следственных действий.

При этом необходимо также выявить обстоятельства, способствовавшие совершению данного преступления. По итогам следствия надлежит установить недостатки общего состояния охраны информационной безопасности в процессе эксплуатации компьютерных систем или сетей, а также причины и условия, способствовавшие нарушению правил их использования (неисправность компьютерного оборудования, отклонение от технического задания и технического проекта, несоответствие средств информационной защиты предъявляемым требованиям — отсутствие сертификата на них). Много обстоятельств, способствовавших нарушению правил эксплуатации ЭВМ, можно установить по материалам служебного расследования, а также по результатам судебных экспертиз (в основном комплексных).

Проведенное нами исследование показывает, что наиболее распространенными поводами к возбуждению уголовного дела по указанным составам преступлений являются: сообщения должностных лиц организаций или их объединений (40 %); заявления граждан (35 %); непосредственное обнаружение органом дознания, следователем или прокурором сведений, указывающих на признаки преступления (20 %); сообщения в средствах массовой информации и иные поводы (5 %) (Приложение А).

По оценкам ведущих зарубежных и отечественных специалистов 90 % компьютерных преступлений остаются необнаруженными или о них не сообщается в правоохранительные органы по различным причинам [78, с. 44; 131, с. 26].

3.2 Тактические особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Рассмотрение особенностей проведения отдельных следственных действий по делам о преступлениях, совершенных в сфере высоких информационных технологий является необходимостью структурного характера диссертации. Такая необходимость определяется индивидуальностью методики расследования

каждого вида преступления, выражающаяся и в особенностях проведения отдельных следственных действий.

В связи с тем, что уже имеется ряд работ А. Н. Васильева [132; 133], А. В. Дулова [134], Н. В. Бахарева [135], Н. И. Порубова [136], Ф. В. Глазырина [137], А. Р. Ратинова [138] и других, посвященных общим вопросам тактики проведения отдельных следственных действий, в этой части работы мы решили отказаться от рассмотрения общих условий производства действий при расследовании преступлений в сфере высоких информационных технологий и остановимся только лишь на наиболее значимых организационно-тактических и криминалистических аспектах проводимых следственных действий.

Общее изучение сущности рассматриваемого вопроса предполагает анализ следующих следственных действий, чье проведение характерно для первоначального этапа расследования по делам о преступлениях, совершенных в сфере высоких информационных технологий:

По мнению Э. Мелик, целями следственных действий при расследовании данного вида преступлений могут являться:

– осмотр и изъятие компьютерной техники;

– поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ЭВМ и ее устройствах;

– поиск и изъятие информации и следов воздействия на нее вне ЭВМ [82].

Полагаем, что указанные цели усекают перечень следственных действий, производство которых возможно при расследовании преступлений в сфере высоких информационных технологий, проводимых с целью установления обстоятельств, имеющих значение для дела. В связи с чем, считаем необходимым, расширить перечень указанных целей и дополнить их, изложив в следующей редакции: целями следственных действий, проводимых при расследовании и раскрытии преступлений в сфере высоких информационных технологий, являются:

– установление и уточнение обстоятельств происшедшего события (способ, место, время, личность совершившего преступное посягательство и пр.);

– выявление, фиксация, изъятие и оценка следов преступления (как традиционных криминалистических, так и нетрадиционных — информационных следов преступлений в сфере высоких технологий), различных вещественных доказательств;

– получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по делу;

– поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ЭВМ и ее устройствах;

– поиск и изъятие информации и следов воздействия на нее вне ЭВМ;

– обнаружение предметов и объектов преступлений;

– осмотр и изъятие компьютерной техники;

– установление лиц, способствующих совершению преступления;

– определение принадлежности компьютерной информации;

– проверка и оценка следственных версий;

– установление причин и условий, способствовавших совершению преступления;

– получение новых доказательств.

Таким образом, приступая к непосредственному исследованию особенностей проведения отдельных следственных действий при расследовании преступлении в сфере высоких информационных технологий (исходя из указанных целей), мы выделяем следующие виды следственных действий, чье рассмотрение будет осуществлено далее: осмотр (включая несколько его разновидностей), обыск и выемка, допрос, следственный эксперимент, предъявление для опознания, назначение экспертиз.

По своей сути, все перечисленные действия могут быть проведены как на первоначальном этапе расследования преступлений в сфере высоких информационных технологий, так и на последующем. Данный факт определяется конкретными условиями расследования преступления. Вместе с тем, исследование сущности установления события преступления и лица его совершившего свидетельствует о том, что успешность проведения перечисленных действий и определяет достижение задач, направленных на быстрое и полное раскрытие преступления, изобличение и привлечение к уголовной ответственности лиц, его совершивших.

Рассматривая следственные действия, производство которых осуществляется при расследовании преступлений указанной категории, еще раз отметим, что проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Осмотр. ***Следственный осмотр*** — это следственное действие, состоящее в непосредственном восприятии, анализе и фиксации следователем или лицом, проводящим дознание, различных материальных предметов и отдельных их элементов в целях обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а также иных обстоятельств, имеющих значение для дела [139, с. 340]. Цель осмотра места происшествия по делам указанной категории — установление конкретного СВТ, выступающего в качестве предмета и(или) орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра — к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра. Исследование специфики следственного осмотра производится, исходя из этапов его производства: подготовительного, рабочего, заключительного.

1. *Подготовительный этап.*

В процессе подготовки к проведению этого следственного действия [78; 140; 141; 142; 143], еще до выезда на место происшествия необходимо решить ряд организационных вопросов, которые в последующем обеспечат качество проведения осмотра места происшествия [144, с. 18].

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, необходимо предварительно провести следующую работу:

– с учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре;

– определить последовательность действия лиц при осмотре места происшествия;

– пригласить соответствующих квалифицированных специалистов;

– подготовить соответствующую компьютерную технику и программное обеспечение, которые будут использоваться для считывания и хранения изъятой информации, при обнаружении изменений в компьютерной информации, исследовании полученной информации, обнаружении информационных следов преступления;

– перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;

– провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

При осмотре места происшествия в состав следственно-оперативной группы (СОГ) в зависимости от конкретной следственной ситуации должны входить следующие лица [105, с. 35]:

– следователь, специализирующийся на расследовании уголовных дел рассматриваемой категории — руководитель СОГ;

– специалист-криминалист, знающий особенности работы со следами преступлений данной категории;

– сотрудник оперативно-технического подразделения правоохранительного органа;

– специалист по сетевым технологиям СВТ (в случае наличия на месте происшествия периферийного оборудования удаленного доступа или локальной компьютерной сети);

– специалист по системам связи (при использовании для дистанционной передачи данных каналов электросвязи);

– оперативные сотрудники;

– участковый инспектор, обслуживающий данную территорию;

– инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, являются охраняемыми объектами).

При необходимости для участия в осмотре места происшествия могут быть приглашены и другие незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и сетей — сотовых, пейджинговых, Интернет и др., и т. д.).

Особенности выбора специалиста. Характерной чертой преступлений в сфере высоких информационных технологий является то, что при проведении

большинства следственных действий необходимо участие специалиста. Как справедливо отмечают Е. Р. Россинская и А. И. Усов, при расследовании преступлений, сопряженных с использованием компьютерных средств, участие специалиста необходимо, поскольку даже малейшие неквалифицированные действия с компьютерной системой зачастую заканчиваются безвозвратной утратой ценной розыскной и доказательственной информации [11, с. 64].

Опрос следователей и специалистов в области вычислительной техники показал, что только 30 % следователей с компьютером на «ты», 14 % следователей работают на ЭВМ на уровне пользователя, 56 % не знают ничего о принципах работы ЭВМ (Приложение Б). При этом, факторами, препятствующими эффективному осуществлению расследования преступлений в сфере высоких информационных технологий, могут выступать как то — недостаточные специальные знания сотрудников, недостаточная оснащенность техникой, несовершенная регламентация правовой нормы или иные факторы (например, установление самого факта нарушения правил эксплуатации ЭВМ, когда потерпевший обычно не выказывает особой заинтересованности в поимке преступника и др.) (рисунок 6).

С другой стороны, 92 % из числа опрошенных программистов считают, что на современном уровне развития вычислительной техники без участия профессионала найти «спрятанную» в компьютере информацию без риска уничтожения сложно. «При этом следователю всякий раз необходимо убедиться в компетентности специалиста» [78, с. 17].

При расследовании преступлений в сфере высоких информационных технологий основными задачами специалистов в области компьютерной техники являются: выполнение всех манипуляций с компьютерной техникой (включение-выключение, разборка-сборка и пр.); оказание помощи следователю в описании компьютерной техники и периферийного оборудования в протоколах следственных действий; проведение экспресс-анализа компьютерной информации; обнаружение информационных следов преступления; предотвращение уничтожения или повреждения компьютерной информации; изъятие компьютерной информации и др.

Следует отметить, что информационные технологии достаточно разнообразны и выбор специалиста для решения конкретных задач расследования может быть весьма сложен. При решении в ходе следственных действий задач, связанных с изъятием технических средств, может быть полезен специалист, знающий элементы и устройства вычислительной техники и систем управления, знакомый с вопросами функционирования автоматизированных систем управления. Для установления фактов проникновения извне в информационные системы специалист должен обладать познаниями в области программного обеспечения вычислительных систем и организации вычислительных процессов, а также обязан знать основы методов защиты информации и информационной безопасности. При исследовании систем ЭВМ и их сетей специалист должен иметь специализацию в области математического и программного обеспечения вычислительных комплексов, систем и сетей, ему также необхо-

димы познания в области компьютерных сетей, узлов связи и средств коммуникаций, организации и распределения информационных потоков.

Поиск таких специалистов следует проводить заблаговременно на предприятиях, в учреждениях, фирмах и компаниях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, разработку программного обеспечения, средств защиты компьютерной информации. Необходимые специалисты могут быть приглашены из учебных заведений и научно-исследовательских организаций, а также из органов внутренних дел. Поскольку отдельные виды судебно-технологических экспертиз проводятся в экспертных подразделениях ОВД на региональном уровне, то производящие их лица также могут быть приглашены в качестве специалистов. В исключительных случаях, могут быть приглашены в качестве специалистов сотрудники организации, компьютеры которой подверглись вторжению.

Понятые. В качестве понятых рекомендуется приглашать людей, сведущих в компьютерной технике [145, с. 73; 146, с. 91]. Непонимание смысла происходящего для человека, приглашенного в качестве понятого, а позднее допрошенного в суде, может не убедить суд в признании тех или иных обстоятельств доказательствами. Понятых в отдельных случаях можно приглашать из числа служащих того предприятия, организации, учреждения, фирмы, компании, в которой проводится осмотр места происшествия, при условии, что они не заинтересованы в исходе дела. В любом случае, поскольку объектом осмотра выступает дорогостоящее оборудование, осмотр места происшествия целесообразно производить в присутствии руководства предприятия, организации, учреждения, фирмы, компании.

Подготовка соответствующей компьютерной техники и программного обеспечения. Это может быть персональный компьютер, исполненный в переносном варианте «Notebook». Кроме компьютера, необходим кабель, а также специальное программное обеспечение, позволяющее осуществлять копирование и экспресс-анализ информации на месте. Следует иметь в виду, что для полного и качественного копирования информации необходимо соответствие не марок компьютеров, а объемов используемых жестких дисков (у переносного компьютера этот объем должен быть не меньше, а в идеальном случае равен объему диска осматриваемого компьютера). Помимо переносного компьютера типа «Notebook», при производстве осмотра могут быть использованы иные носители информации, обладающие большой емкостью: лазерные и DVD диски, ZIP-накопители и др.

При *инструктаже членов следственно-оперативной группы* особое внимание необходимо уделить их поведению во время осмотра: внимательно следить за поведением всех лиц, которые могут находиться в помещении, где производится осмотр; проявлять особую осторожность при обращении с компьютерной техникой, создавая условия для работы с ней специалисту. Следует помнить, что компьютерная техника — это дорогостоящее оборудование, которое требует осторожности при обращении с ней, в том числе и при ее изъятии. К тому же она может хранить значительное количество информации, являющейся собственностью, как отдельного лица, так и фирмы. Единственная ошибка может привести к миллионным убыткам. В ходе инструктажа участников следственно-

оперативной группы следователь указывает основные задачи предстоящего следственного действия, особенности его производства по рассматриваемому виду преступлений, указывает на характер действий каждого лица. Представляется обоснованным такой инструктаж проводить следователю в паре со специалистом. При этом необходим категорический запрет кому бы то ни было из лиц, работающих на объекте осмотра или находящихся на нем по иным причинам, соприкасаться с ЭВМ, выключать без специального указания со стороны следователя энергоснабжение объекта, самостоятельно производить какие-либо манипуляции со средствами компьютерной техники, если результат этих манипуляций заранее не известен.

Как показывает опрос респондентов (в 60 % случаев), при изъятии средств компьютерной техники у следователя могут возникать конфликты с персоналом. При их разрешении дополнительно к вышеизложенным правилам желательно руководствоваться следующими рекомендациями:

1) недопустимо производить изъятие в несколько приемов, даже если следователь не располагает необходимым транспортом. В этом случае нужно сделать несколько рейсов с объекта до места хранения изъятых материалов;

2) изъятые материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица;

3) недопустимо оставление на объекте части средств компьютерной техники по мотивам ее «абсолютной необходимости» для деятельности данной фирмы (организации). Желание персонала сохранить от изъятия определенные СКТ — обычно указывает на наличие на них важной для следствия информации;

4) следует изымать все СКТ, находящиеся в помещении объекта, независимо от их юридической принадлежности;

5) если персонал настаивает на отражении в протоколе следственного действия конкретных качеств изымаемых СКТ (марка, быстродействие, марка процессора, объем памяти и т. д.), то эти сведения могут быть записаны лишь как отдельные заявления.

2. *Рабочий этап.*

Прежде чем приступить к осмотру, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Общими правилами обращения с вычислительной техникой и носителями информации являются:

– все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством;

– применение средств криминалистической техники — магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ЭВМ, должно быть согласовано со специалистом;

– необходимо исключить попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.);

– при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок);

– диапазон допустимых температур при хранении и транспортировке должен варьироваться в температурных пределах от 0 до + 50 градусов Цельсия;

– со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

По прибытию на место происшествия, следователь должен:

1) удалить с места происшествия всех посторонних лиц и организовать его охрану, если этого не было сделано. Обязательной охране подлежат: территория места происшествия; все СВТ, находящиеся на территории (в помещении); пункты отключения электропитания СВТ, находящиеся в здании (учреждении, организации, на территории);

2) зафиксировать обстановку, сложившуюся на момент осмотра места происшествия, произвести ориентирующую и обзорную фото-, видеосъемку;

3) исключить возможность посторонним лицам (да и участникам следственно-оперативной группы) соприкасаться с оборудованием. Желательно лишить их возможности пользоваться телефоном, а при острой необходимости делать это только с разрешения следователя. «Не допускайте, чтобы кто-либо производил любые действия с компьютером. Риск, связанный с непосредственным вмешательством в систему, значительно больше, чем малый шанс дистанционного влияния на систему с другого устройства» [147, с. 16]. Необходимо организовать охрану каждого компьютера (терминала), для чего возможно привлечение дополнительных сил (подразделений ОВД и пр.);

4) опросить потерпевшего, материально ответственное лицо и очевидцев (операторов СВТ) об изменениях, внесенных в обстановку, о категории обрабатываемой информации (общедоступная или конфиденциальная), а также о действиях потерпевшего до прибытия СОГ. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств;

5) определить, соединены ли находящиеся в помещении компьютеры в локальную вычислительную сеть. На это могут указать коаксиальные кабели, идущие от компьютера к компьютеру, или просто телефонные провода. При наличии локальной компьютерной сети наибольший интерес представляет центральный компьютер, так называемый сервер, на котором хранится большая часть информации и к которому имеют доступ все ЭВМ. Этот компьютер необходимо обследовать более тщательно и осторожно;

6) установить, имеются ли соединения компьютера с оборудованием или вычислительной техникой вне осматриваемого помещения. На это могут указывать кабели и провода, идущие от компьютера в другие помещения или зда-

ния. Если есть соединения, то существует реальная возможность непосредственного обмена информацией, независимо от желания специалиста, ее изменения или уничтожения с удаленных рабочих мест, находящихся за несколько метров или даже километров от обыскиваемого помещения. Для предотвращения этого на время съема информации вычислительную сеть необходимо отключить от «внешнего мира» программно или физическим отключением кабелей. Эту работу квалифицировано может выполнить только специалист в области вычислительной техники;

7) выяснить, подключен ли компьютер к телефонной линии. В случае подключения на него могут поступать вызовы с дальнейшими приемами или передачами информации. Следует иметь в виду, что установить — запрограммирован ли компьютер на передачу, может только специалист. Если информация, поступающая на компьютер по электронной почте, факсимильной или телетайпной связи может иметь интерес, то отключать телефонную или телетайпную линии нет смысла, но необходимо воздерживаться от телефонных разговоров по данной линии;

8) определить, запущены ли программы на ЭВМ и какие именно. Для этого необходимо изучить изображение на экране и, по возможности, детально описать его в протоколе. Если специалисту удастся определить, что на компьютере работает программа уничтожения информации или ее зашифровки, то такие программы стоит приостановить и обследование начать именно с этого компьютера. Важно отметить, что следователю в любом случае не следует самому производить какие-либо манипуляции с вычислительной техникой. Их должен осуществлять специалист.

На рабочей (исследовательской) стадии осмотра места происшествия каждый объект подлежит тщательному обследованию. В этот период времени важно установить, не содержится ли на компьютере информация, которая может способствовать более плодотворному и целенаправленному осмотру (различные планы помещений, участков местности, пароли, коды доступа, шифры и т. п.). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого дисков. Интерес могут представлять также файлы с текстовой или графической информацией. Также следует обращать внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройств на них.

В этот период осмотра фиксируется текущее состояние компьютерной информации, делается вывод о произошедшем событии и его последствиях: уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, их системы или сети; устанавливается способ совершения преступления. Для этого с помощью специалиста наблюдается действие программ, содержимое текстовых файлов и баз данных. При этом особое внимание следует уделить изучению имеющихся в большинстве компьютерных систем файлов регистрации. Какое бы событие не произошло в системе, информация о нем (в том числе, кто инициировал его, когда и в какое время оно произошло, какие

при этом были затронуты файлы) регистрируется в этих файлах. В частности, в файлах регистрации может получить отражение информация о паролях пользователей, их именах, идентификационных номерах. В последствии данная информация может быть использована для установления компьютера, с которого произошел неправомерный доступ к компьютерной информации.

В протоколе осмотра следует отразить следующие фактические данные:

– наименование и назначение объекта, где совершено преступление;

– территориальное расположение объекта осмотра (на улице, в помещении, в банке, в магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т. д.) и его ориентация относительно сторон света;

– ближайшее окружение объекта и подступы к нему — здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в т. ч. и водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцев, концентраторов т. д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло-, водо- и газоснабжения, вентиляции и т. д.);

– технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и состояние электрооборудования и др.);

– наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации — постов охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещения, металлических решеток, штор, жалюзи, рольставен, замков и запорных механизмов, экранов, заземлений, специальных стекол и пленок, генераторов шума, фильтров и т. д.;

– расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

– расположение в одном помещении вместе с СВТ других электрических устройств и приборов — телефонных и иных аппаратов электросвязи, систем электрочасофикации, оргтехники (ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок и т. п.), приборов электроосвещения (настольных, напольных, настенных, потолочных, подвесных и т. д.), абонентских громкоговорителей, телевизоров и мониторов, радиоприемников и магнитол, электроплиток, печей, чайников, кондиционеров и т. д.;

– наличие в одном помещении с СВТ линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенны-провода, водо- и газоснабжения);

– наличие или отсутствие технических средств сопряжения СВТ с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми СВТ соединены между собой, а также с аппаратами или линией электросвязи);

– наличие или отсутствие соединений СВТ с оборудованием или вычислительной техникой, находящейся вне территории (помещения) осмотра; на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется);

– наличие на объекте, путях подхода и отхода следов преступления и преступника, специфическими среди которых являются: следы орудий взлома, повреждения, уничтожения и(или) модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли; следы проплавления, прокола, надреза изоляции проводов СВТ, наличие участков механического сдавливания и приклеивания сторонних предметов;

– наличие или отсутствие учетно-справочной документации к СВТ — технического паспорта и подобного ему документа; журнала оператора или протокола автоматической фиксации расчетно-кассовых и иных операций; журнала учета машинных носителей информации (МНИ), машинных документов, заказов (заданий или запросов); журнала (карточки) учета выдачи МНИ и машинных документов; журнала (карточки) учета массивов (участков, зон), программ, записанных на МНИ; журнала учета уничтожения брака бумажных МНИ и машинных документов; актов на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов.

Непосредственно в ходе осмотра компьютерной техники следует принимать во внимание следующие неблагоприятные факторы:

– возможные попытки со стороны персонала повредить ЭВМ с целью уничтожения информации и ценных данных;

– возможное наличие на компьютере специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

– возможное наличие на ЭВМ иных средств защиты от несанкционированного доступа;

– постоянное совершенствование компьютерной техники, следствием чего может быть наличие на объекте программно-технических средств не знакомых следователю и специалисту.

В связи с чем необходимо предвидеть «меры безопасности», предпринимаемые преступниками с целью уничтожения вещественных доказательств. Ими может, например, использоваться специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал магнитное поле в дверном проеме такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты. Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер требовать пароль периодически и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожатся. Изобретательные владельцы компьютеров устанавливают иногда скрытые команды, удаляющие или архивирующие с паролями важные данные, если некоторые процедуры запуска машины не сопровождаются специальными действиями, известными только им [148, с. 149].

В целях недопущения вредных последствий перечисленных факторов следователь должен придерживаться следующих рекомендаций:

– перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель приводит к потере информации в оперативной памяти и даже к частичному стиранию информационных ресурсов на данном компьютере) [11, с. 399-411; 149, с. 16-21];

– принять меры к установлению пароля доступа в защищенных программах;

– при необходимости консультаций у персонала предприятия получать их у разных сотрудников данного отдела путем опроса порознь. Такой метод позволит получить максимально правдивую информацию и избежать преднамеренного вредительства;

– при нахождении ЭВМ в локальной вычислительной сети необходимо иметь бригаду специалистов для быстрого реагирования на движение информации по сети;

– наряду с осмотром компьютера, обеспечить осмотр документов о пользовании им, в которых следует обратить особое внимание на рабочие записи операторов ЭВМ, так как часто именно в этих записях неопытных пользователей можно обнаружить коды, пароли и другую очень ценную для следствия информацию. При осмотре должен присутствовать кто-либо из сотрудников предприятия, способный дать пояснения по установленному на ЭВМ программному обеспечению. Если на начальной стадии осмотра не удалось установить пароли и коды используемых программ, то компьютер подлежит опечатыванию и выемке, с тем чтобы в последующем в стационарных условиях прокуратуры или лаборатории с привлечением специалистов-программистов выявить существующие пароли и коды доступа, осуществить надлежащий осмотр компьютера и

содержащихся на нем файлов. В таких случаях достаточно изъять только системный блок, в который входят процессор и накопители на магнитных дисках. Остальную часть компьютера (монитор, клавиатуру, принтер) следует опечатать.

Кроме того, как отмечает ряд ученых, необходимо соблюдение также следующих рекомендаций:

– недопустимо производить изъятие в несколько приемов. В том случае, если следователь не располагает необходимым транспортом, следует сделать несколько рейсов от объекта до места хранения изъятых материалов с выставлением охраны на объекте изъятия (охране подлежат неизъятые СВТ и помещение, в котором они находятся);

– изъятые предметы и материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица;

– недопустимо оставлять на объекте части СВТ по причине их «абсолютной необходимости» в деятельности данного пользователя: как правило, желание сохранить от изъятия определенные СВТ указывает на наличие в них важной для следствия информации;

– следует изымать все СВТ, находящиеся в помещении объекта и несущие следы преступной деятельности;

– в протоколе следственного действия должны обязательно фиксироваться конкретные признаки изымаемых СВТ (марка, быстродействие, марка процессора, объем памяти и т. д.) [150, с. 92].

3. *Заключительный этап.*

Изъятие средств компьютерной техники производится только в выключенном состоянии. При этом должны быть выполнены и отражены в протоколе следующие действия:

– установлено включенное состояние оборудования и зафиксирован порядок его отключения;

– описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов);

– описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация);

– определено отсутствие либо наличие компьютерной сети, используемый канал (каналы) связи и телекоммуникаций. В последнем случае установлен тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

– произведено разъединение (с соблюдением всех необходимых мер предосторожности) аппаратных частей (устройств) с одновременным опломбированием их технических входов и выходов;

– определен вид упаковки и транспортировки изъятых предметов.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия металлодетекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры. Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранении изъятых объектов решается следователем в каждом конкретно случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса.

Осмотр средств вычислительной техники (СВТ), участвовавших в преступлении, производят для достижения следующих целей:

– обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для установления, кем, с какой целью и при каких обстоятельствах было совершено преступление;

– выяснения обстановки происшествия для восстановления механизма совершения преступления;

– установления технического состояния СВТ.

При реализации первой цели требуется участие специалиста-криминалиста и специалиста в области СВТ и информационных технологий. В решении двух других непосредственное участие специалиста-криминалиста не требуется. В зависимости от специфики осматриваемого СВТ в следственном действии должны принимать участие следующие специалисты:

– по обслуживанию и ремонту СВТ (для осмотра аппаратной части СВТ и соединительной арматуры; для ЭВМ — инженер-системотехник);

– в области сетевых технологий (для осмотра СВТ, используемых в системах дистанционной передачи данных — компьютерных сетях, периферийного оборудования удаленного доступа, удаленных терминалов);

– по средствам связи и телекоммуникациям (для осмотра оборудования электросвязи, используемого для передачи компьютерных данных и команд, а также СВТ, являющихся средствами связи);

– инженер-программист (для осмотра программного обеспечения СВТ, определения принципа его функционирования, установления следов преступной деятельности в среде машинной информации).

В протоколе осмотра СВТ фиксируются следующие данные:

– тип, марка, конфигурация, цвет и заводской номер (или инвентарный, учетный номер) изделия;

– тип (назначение), цвет и индивидуальные признаки соединительных и электропитающих проводов;

– состояние СВТ на момент проведения осмотра (выключено или включено);

– техническое состояние — внешний вид, целостность корпуса, комплектность СВТ — наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой, наличие расходных материалов, тип используемого машинного носителя информации и т. д. (проверку проводит соответствующий специалист);

– тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенных к нему электроприборов, число разъемов-розеток и т. д.);

– наличие заземления («зануления») СВТ и его техническое состояние;

– наличие и техническая возможность подключения к СВТ периферийного оборудования и(или) самого СВТ к такому оборудованию либо к каналу электросвязи (определяется специалистом по наличию у СВТ соответствующих портов и разъемов);

– повреждения, непредусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его деталей (частей, блоков), особенно те, которые могли возникнуть в результате происшествия или преступления, а также спровоцировать создание внештатной технической ситуации (привести к возникновению происшествия);

– следы преступной деятельности (орудий взлома корпуса СВТ, проникновения внутрь корпуса СВТ, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств, а также канифоли, припоя, флюсов и других химических веществ, обрезки монтажных проводов и изоляционных материалов, кровь, пот, волосы, волокна ткани и т. д.);

– расположение СВТ в пространстве относительно периферийного оборудования и других электротехнических устройств;

– точный порядок соединения СВТ с другими техническими устройствами;

– категорию информации, циркулирующей в СВТ (общедоступная или конфиденциальная);

– наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа;

– расположение рабочих механизмов СВТ и изображение на его экране (мониторе) или визуально-контрольном окне (для принтеров, контрольно-кассовых машин, контрольно-пропускных механизмов, цифровых аппаратов связи и т. д.) в том случае, если на момент осмотра они находятся в рабочем состоянии;

– все основные действия, производимые специалистом при осмотре СВТ (порядок нажатия на клавиши и запорные механизмы, корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения или соединения СВТ и ее составляющих, отсоединения коммуникационных и электропитающих

проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т. п.).

Осмотр машинного носителя информации (МНИ) может быть произведен в ходе осмотра места происшествия или как самостоятельное следственное действие.

Осмотр МНИ производится с участием специалиста и начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием. К машинным носителям информации, как правило, относятся магнитные диски (гибкие — дискеты, жесткие — «винчестеры», «банки» и «Zip»); оптические и магнитооптические компакт-диски (CD — «лазерные диски»); пластиковые карты (карточки); интегральные микросхемы (ИМС), в т. ч. находящиеся в различных СВТ — в виде оперативной памяти (ОЗУ) и(или) постоянного запоминающего устройства (ПЗУ) — персональных компьютерах, сотовых и иных аппаратах электросвязи, электронных записных книжках, электронных переносных справочниках и переводчиках, контрольно-кассовых аппаратах, банкоматах, контрольно-пропускных устройствах, смарт-картах и т. д.).

В протоколе осмотра должны быть зафиксированы следующие фактические данные:

1. Тип, вид, марка, назначение, цвет и заводской номер (или учетный номер носителя).

2. Наличие индивидуальных признаков и техническое состояние футляра (коробки, упаковки, специального технического устройства) — тип, размеры, цвет, материал, физические повреждения, наклейки, принцип функционирования, емкость и т. д.

3. Техническое состояние — размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность (механические повреждения — царапины, деформации, нарушения несущего слоя и т. д.), наличие и положение (сохранность) приспособлений от несанкционированного уничтожения (перезаписи) информации (ключей, пломб, заглушек, маркеров), наличие и техническое состояние механизмов защиты информационно-несущего материала (отверстий окон для считывания и записи информации).

4. Наличие, размеры, цвет, марка и техническое состояние разъемов для подключения к специальному считывающему устройству.

5. Присутствие внешней спецификации, ее цвет и размеры (заводские или пользовательские наклейки с текстом или специальными пометками).

6. Наличие индивидуальных признаков защиты носителя от несанкционированного использования (тип — голография, штрих-код, флюоресцирование, перфорация, ламинирование, вплавление личной подписи пользователя и т. д.; размеры, цвет, вид).

7. Признаки материальной подделки МНИ и их защиты — подчистки, подтирки, травления, термическое воздействие, переклеивание (склеивание, наклеивание, заклеивание), дописки, замены, перепайки и т. д.

8. Работоспособность и внутренняя спецификация — серийный номер и(или) метка тома, либо код; размер разметки (для дисков — по объему записи информации, для лент — по продолжительности записи); размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных программ, файлов, каталогов (подкаталогов), данных, их структура, название (имя и(или) расширение), размер и объем, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т. д.); наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения).

9. Результат осмотра содержимого файлов (программ, компьютерной информации), записанных на МНИ или находящихся в оперативной памяти СВТ и имеющих значение для дела.

10. Все манипуляции (нажатия на клавиши и т. д.) со средствами вычислительной техники, совершенные в процессе осмотра.

11. Индивидуальные признаки СВТ, используемые в процессе осмотра, — тип, вид, марка, название, заводской или регистрационный (учетный) номер и т. п.

12. Ссылка на то, что используемые в процессе осмотра СВТ перед началом следственного действия были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

Осмотр машинного документа.

Документ — материальный объект, созданный человеком для закрепления, передачи, обработки и хранения информации [22, с. 35]. Для осмотра важно то, что носители информации, отраженной в документе, могут быть разнообразными. Документы могут иметь вид текста, звукозаписи, изображения. Документы имеют целевые характеристики — передача во времени, в пространстве, хранение (запоминание), общественное использование. Они отражены в содержании документа. В компьютерных (автоматизированных) системах документ — любой объект, находящийся в памяти компьютера. В условиях развития «высоких технологий» возникают принципиально новые носители информации, совершается постепенный переход к «бездокументарному управлению» — без традиционного бумажного документа. Эти явления могут использоваться в преступных целях. Возникает потребность совершенствования средств обнаружения новых документов, закрепленных на нетрадиционных носителях, и, в случае необходимости, их изъятия, прочтения и осмотра.

Осмотр документа на машинном носителе и машинограмме, создаваемым СВТ, производится с участием специалиста (или группы специалистов) в зависимости от сферы (области) деятельности, в которой используется осматриваемый документ (кредитно-финансовая, банковская, расчетно-кассовая, услуг, охраны и т. д.).

Цели осмотра — выявление и анализ внешних признаков и реквизитов документа, анализ его содержания, обнаружение возможных признаков его подделки (фальсификации).

В протоколе осмотра документа должны быть отражены следующие данные:

1. Наименование (назначение) документа (например, идентификационный код и наименование формы документа по классификатору [151]).

2. Тип используемого машинного носителя, его индивидуальные признаки и техническое состояние.

3. Тип, марка, конфигурация и техническое состояние аппаратного и программного оборудования, других технических устройств, применявшихся при осмотре.

4. Наличие сопроводительного письма или документа, его заменяющего (например, договора на использование пластиковой карточки или регистрационного сертификата на использование электронно-цифровой подписи [152]).

5. Форма записи содержания документа (человекочитаемая, закодированная в машинном формате, смешанная).

6. Реквизиты организации (лица) создателя документа (наименование и юридический адрес).

7. Наличие грифа ограничения доступа к документу на машинном носителе или машинограмме («конфиденциально», «для служебного пользования», «секретно», «совершенно секретно»).

8. Регистрационный номер документа и(или) машинного носителя (заводской номер, серийный номер тома, метка тома).

9. Дата изготовления (создания) или выдачи документа (с указанием времени записи документа на МНИ, позволяющим идентифицировать ее с машинным протоколом).

10. Размер документа (линейный или объемный — по количеству символов или общему объему символов в документе в байтах) и(или) количество страниц.

11. На чье имя выдан (реквизиты адресата-получателя).

12. Какими реквизитами заверен (электронно-цифровой подписью; кодом (позывным) лица, ответственного за правильность изготовления, копирования или передачу документа по телекоммуникационным каналам; собственноручной подписью уполномоченного лица; печатью; индивидуальным кодом абонента сети дистанционной передачи данных — «электронной почты»; специальным позывным кодом аппаратуры связи).

13. Индивидуальные признаки документа (название файла-программы); структура расположения символов; машинный формат текста (формат MS DOS, WORD for WINDOWS и т. д.); наличие маркеров страниц, выделений текста; тип и цвет печати (матричный, струйный, электрографический, смешанный) указать конкретно для каждого элемента; наличие защитных знаков и т. д.).

14. Выявленные при осмотре признаки подлога и материальной подделки документа и его носителя.

В заключении рассмотрения вопроса об особенностях производства осмотра, при расследовании преступлений в сфере высоких информационных технологий отметим, что:

– стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных со СВТ, средствами и системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровня их соподчиненности и используемых средств связи и телекоммуникации во избежание их разрушения, нарушения заданного технологического ритма и режима функционирования причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств;

– осмотр места происшествия, средства вычислительной техники, машинного носителя информации и документа необходимо проводить в строгой последовательности, уделяя особое внимание тем частям предметов, на которых имеются повреждения и следы, и с обязательным использованием фото- и(или) видеосъемки. Важно сфотографировать или произвести видеозапись не только места происшествия, отдельных объектов, СВТ и их соединений, но и все действия специалистов, участвующих в осмотре;

– к протоколу осмотра прилагаются план или схема места происшествия, принципиальная схема соединения СВТ между собой и с каналами электросвязи (со спецификацией и расшифровкой условных обозначений), фото-, видеопленка или магнитный носитель информации (лента, дискета или жесткий диск), распечатка наиболее значимой для следствия информации на бумаге.

Обыск, выемка.

В теории науки криминалистики обыск — следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка — следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю [153, с. 290].

Задачами обыска [24; 154; 155; 156] при расследовании преступлений в сфере высоких информационных технологий являются отыскание и изъятие:

1) орудий, используемых для совершения преступления в сфере компьютерной информации, в том числе носителей информации, примененных для копирования похищенной информации или содержащие программы «взлома» защиты компьютера, вредоносные программы, иные программы и файлы данных (например, библиотеки паролей и имен), использованные при совершении преступления;

2) компьютерной информации;

3) специальной литературы, посвященной вопросам компьютерной безопасности, эксплуатации ЭВМ, создания вредоносных программ, неправомер-

ного доступа к компьютерной информации, принципов и алгоритмов организации компьютерных сетей, программного обеспечения и пр.;

4) иных вещественных доказательств и документов, имеющих значение для дела;

5) разыскиваемого лица.

Поскольку одним из основных процессуальных способов изъятия вещественных доказательств является обыск, целесообразно уделить особое внимание не только самому факту его проведения, но и процессу подготовки к нему (разумеется, в случаях, когда такая возможность имеется). Как показывает практика, среду, в которой проводится обыск, можно разделить на два вида — «агрессивная», когда рассчитывать на содействие сотрудников или владельцев не приходится, и «позитивная» — когда собственник заинтересован в установлении истины.

В первом случае подготовка к обыску должна базироваться в основном на материалах оперативных разработок. Сам факт возможного проведения обыска должен оставаться непредсказуемым для подозреваемого до последнего момента, для исключения возможности уничтожения следов.

Во втором случае подготовка может быть более проработана. Необходимо получить схему проводки локальной вычислительной сети с покабинетной расстановкой компьютеров. По информации файлового сервера в режиме реального времени установить, кто и с какой задачей работает в настоящий момент, после этого проводить обыск на рабочем месте. Если имеется возможность, целесообразно заблаговременно установить специальную технику. Это позволит задержать преступника с поличным.

На подготовительной стадии следователь должен решить ряд вопросов организационного характера. Необходимо получить максимум информации об условиях и обстановке места, где предстоит произвести обыск. Для получения указанных данных может быть использована как доказательственная, так и непроцессуальная информация [157, с. 41]. В процессе планирования обыска следователь собирает необходимую информацию и решает конкретные задачи:

1. Сбор сведений об искомых объектах. Подробно выясняются вид и содержание информации, которая предположительно могла попасть к обыскиваемому преступным путем; характер вредоносных программ, вирусов; программные средства, которые в состоянии определить их наличие, и пр. Выясняется, на каком типе носителей машинной информации могут содержаться искомые данные. Необходимо также изучить личность владельца компьютера, его профессиональные навыки по владению компьютерной техникой. Если это программист со стажем, то для изъятия и анализа компьютерной информации может понадобиться специальное программное обеспечение для ее поиска, просмотра, распаковки, расшифровки или иного исследования.

2. Ознакомление с местом предстоящего обыска. Необходимо выяснить сведения о помещении (служебное или жилище). Устанавливается точный адрес, расположение и планировка, пути подхода, наличие службы охраны. Выясняется количество и тип компьютерной техники, наличие локальной сети и ее

устройство, количество компьютеров, объединенных в сеть, возможность выхода в Интернет, удаленного доступа, средств защиты информации от несанкционированного доступа (программных и технических), наименование операционной системы. Указанные данные можно получить из документации по строению у провайдера путем оперативно-розыскных мероприятий.

3. Определение времени проведения обыска. Время выбирается с учетом особенностей каждой конкретной ситуации. Как справедливо отмечает А. Н. Иванов, поспешность или медлительность могут оказать негативное влияние на процесс расследования [157, с. 42] (наиболее удачными являются утренние часы — с 6.00 до 8.00). При решении этого вопроса необходимо попытаться обеспечить, прежде всего, внезапность проведения обыска. Внезапность проникновения на место обеспечивается общими тактическими приемами обыска: транспорт оставляется вне возможного поля зрения лиц, находящихся в обыскиваемом помещении; организуется наблюдение за окнами и входом в помещение; подход к дому осуществляется, как правило, несколькими группами, чтобы не вызвать подозрений. Для проникновения в квартиру используют помощь работников коммунальной службы, соседей.

4. Подготовка материально-технического обеспечения. Готовится переносной компьютер, при помощи которого можно будет осмотреть исследуемую информацию, носители машинной информации. Решается вопрос с транспортом и материалами для транспортировки при изъятии оборудования и машинных носителей.

5. Обеспечение необходимых участников обыска. Подбирается соответствующий специалист. В зависимости от обстановки возможно участие двух и более специалистов. По возможности подбираются понятые, обладающие некоторыми познаниями в области компьютерной техники. В случае, когда возможно воспрепятствование проходу следственно-оперативной группе к месту обыска, необходимо решить вопрос о привлечении дополнительных сил и средств.

6. Получение санкции на производство обыска.

По прибытии к месту проведения обыска необходимо вести себя следующим образом:

– быстро и внезапно войти в обыскиваемый объект (или одновременно в несколько помещений);

– при оказании сопротивления со стороны лиц, находящихся на объекте обыска, — обыскиваемого, его родственников, охранников (сторожей), сотрудников организации и т. п. — принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

– организовать охрану места обыска и наблюдение за ним; охране подлежат периметр обыскиваемых площадей, СВТ, хранилища МНИ, все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади), специальные средства защиты от несанкционированного доступа, хранилища ключей аварийного и регламентно-

го доступа к СВТ, помещениям и другим объектам (пульты, пункты, стенды, сейфы и т. п.).

Необходимо отметить, что к изменению или уничтожению машинной информации, ее носителей и СВТ, которые впоследствии могут выступать в качестве доказательств по делу, приводят не только манипуляции с самими СВТ, но и включение или выключение их электропитания. Поэтому все электротехническое оборудование и средства электротехнических систем, имеющиеся на месте обыска, должны находиться до момента их осмотра специалистом в том пространственном положении и техническом состоянии, в котором они были в момент начала обыска [149, с. 15].

На обзорной стадии необходимо:

1. Определить и отключить специальные средства защиты информации и СВТ от несанкционированного доступа, особенно те, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ и машинной информации, порядка их использования и(или) установленных правил работы с ними; принять меры к установлению пароля, ключа санкционированного доступа и шифрования-дешифрования информации.

2. Установить наличие телекоммуникационной связи между СВТ, СВТ и каналами электросвязи по схемам «компьютер — компьютер», «компьютер — управляющий компьютер», «компьютер — периферийное устройство», «компьютер — средство электросвязи», «компьютер — канал электросвязи», «периферийное устройство — периферийное устройство», «периферийное устройство — канал (средство) электросвязи» и наоборот.

При наличии компьютерной сети любого уровня, в первую очередь, должен быть осмотрен и подвергнут обыску центральный управляющий компьютер (сервер сети, компьютер процессингового центра, узла связи, охранной системы и т. п.). Следует обратить внимание на тот факт, что при наличии соединения СВТ с другим оборудованием и электронно-вычислительной техникой, находящимися вне периметра обыскиваемой зоны (в другом помещении, здании, населенном пункте и т. д.), существует реальная возможность непосредственного доступа к машинной информации и совершения любых действий с ней и СВТ (стирание, уничтожение, модификация, копирование, блокирование, нарушение работы). Для предотвращения этого необходимо, в зависимости от ситуации и рекомендаций специалиста, временно или на длительный срок, частично или полностью отключить СВТ или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром обыскиваемой зоны. Отключение может быть произведено как на программном, так и аппаратном уровне. Если СВТ работает в режиме «электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе обыска [158, с. 16].

3. Определить СВТ, находящиеся во включенном состоянии, и характер выполняемых ими операций и(или) программ. Особое внимание необходимо уделить терминальным печатающим и видеоотображающим устройствам (принтерам и мониторам). Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора изучено и детально описано в протоколе (можно также зафиксировать его на видеопленку, либо сделать распечатку на бумаге с использованием специальных сканирующих программ).

Если специалисту удастся установить, что на момент обыска на каком-либо СВТ происходит уничтожение информации, либо уничтожается машинный носитель информации, необходимо всеми возможными способами приостановить этот процесс и начать обследование с данного места или СВТ.

4. При обследовании персонального компьютера необходимо:

– установить последнюю исполненную программу и(или) операцию, а при возможности все, начиная с момента включения компьютера;

– произвести экспресс-анализ машинной информации, содержащейся на жестком диске и в оперативной памяти компьютера с целью получения информации, имеющей значение для следствия (интерес могут представлять файлы с текстовой и графической информацией).

Детальный этап обыска является очень трудоемким и требует высокой квалификации как специалиста в области СВТ, так и всей следственно-оперативной группы.

Необходимо четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться предметы, устройства и документы. Ими может служить и само СВТ — аппаратные и программные оболочки модулей его составляющих. Например, внутри корпуса резервируется место для расширения и наращивания возможностей компьютера путем установки дополнительных плат. Это и приводит к большому объему дополнительного места внутри корпуса системного блока компьютера.

Поскольку наиболее распространенным носителем компьютерной информации являются магнитные дискеты, а они имеют сравнительно малые размеры — до 150 мм в диаметре и 2 мм в толщину, поиск их значительно затруднен. Если нет возможности, чтобы специалист просмотрел дискеты на месте, они должны быть изъяты для дальнейшего исследования (с соблюдением всех процессуальных правил).

Наряду с дискетами для хранения информации могут использоваться лазерные диски, т. к. они внешне не отличаются от аудио- и видеодисков, это делает возможным их хранение среди музыкальной или видеоколлекции.

В связи с тем, что быстро проанализировать огромное количество информации на компьютере не всегда возможно, ее необходимо изъять для дальнейшего исследования. Устройства, на которых произведено копирование, должны быть соответствующим образом упакованы и опечатаны. При этом следует иметь в виду, что нецелесообразно изымать все компьютерное оборудование, находящееся в месте обыска. В криминалистической литературе справедливо

отмечается, что кроме технических сложностей подобного изъятия существуют и экономические: «в случае выхода из строя ЭВМ банк, как правило, может “продержаться” не более двух дней, оптовая фирма — 3-5, компания обрабатывающей промышленности — 4-8, страховая компания — 5-6 дней. В связи с этим, радикальное изъятие компьютерной техники грозит последующими претензиями пострадавших организаций» [159, с. 65].

Следователю стоит придерживаться следующих рекомендаций:

– при невозможности вскрытия корпуса СВТ (если это может привести к утрате информации, физическому повреждению ее носителя либо приведению к неисправному состоянию) необходимо изъять СВТ целиком для лабораторного исследования;

– все обнаруженные машинные носители информации (дискеты, пластиковые карточки, в т. ч. аудио-, видеокассеты и оптические компакт-диски) следует изъять для последующего анализа содержащихся на них данных на аттестованном исследовательском оборудовании, при отсутствии которого осмотр информации недопустим;

– нельзя использовать специальную поисковую и досмотровую технику, один из элементов которой — источник электромагнитных или магнитных излучений (металлодетекторы, магниты, электронные стетоскопы, рентгеновские установки и т. п.), поскольку их применение может привести к стиранию информации на носителях;

– при необходимости изъятия жесткого диска персонального компьютера целесообразно изъять весь процессорный (системный) блок;

– в случае изъятия печатающего устройства (принтера) необходимо помнить, что в настоящее время возможна идентификация печатной продукции, изготовленной лишь на матричном (игольчатом) принтере. Для лазерного (электрографического) и струйного типов принтеров данный анализ практически невозможен.

На заключительном этапе составляются протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения СВТ относительно друг друга, строительных проемов, инженерно-технических коммуникаций, оконечных устройств электронесущей арматуры, а также принципиальная схема соединения СВТ между собой и с другими техническими устройствами; проводятся дополнительная фотосъемка и видеозапись.

При производстве выемки следует придерживаться рассмотренных нами рекомендаций по осмотру, обыску с учетом процессуальной процедуры производства данного следственного действия.

Допрос.

Допрос подозреваемого и обвиняемого. При допросе лица в качестве подозреваемого [139, с. 97; 160, с. 289-291] в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал подозреваемый?; к какой компьютерной информации имеет доступ?; какие операции с информацией он имеет право проводить?; какова

его категория доступа к информации?; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации?; кто научил его работать с конкретным программным обеспечением?; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети)?; к каким видам программного обеспечения имеет доступ подозреваемый?; каков источник его происхождения?; обнаруживались ли программы, источник происхождения которых неизвестен?; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время?; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ?; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации?; как подозреваемому удалось проникнуть в компьютерную систему (сеть)?; откуда подозреваемый мог узнать пароль (код) доступа к информации?».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения?; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети?; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно?; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ?; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации?; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения?; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей?».

Следует иметь в виду, что на первом допросе подозреваемый может попытаться объяснить факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.). Может рассказывать о неправомерном доступе к компьютерной информации, как о факте, который совершился при отсутствии преступного умысла.

Для изобличения таких лиц хорошие результаты дает правильная реализация информации о преступной деятельности этого лица, полученной при проведении оперативно-розыскных мероприятий, а так же предъявление предметов и документов, принадлежащих подозреваемому и использовавшихся для неправомерного доступа к компьютерной информации [161, с. 53]. Умелое использование указанных сведений оказывает определенное воздействие на допрашиваемого и позволяет получить правдивые показания на первом допросе.

Для успешного проведения допроса обвиняемого необходимо тщательно изучить все материалы дела, особенности личности обвиняемого, способы со-

вершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве обвиняемого следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй — что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК [162, с. 10].

Как отмечает ряд авторов, допрос обвиняемого является одним из важнейших, наиболее сложных и зачастую конфликтных следственных действий [163; 164]. Не преследуя цели рассмотрения тактики допроса обвиняемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу доказательств и подробного изложения обстоятельств преступления без ссылки на источники [165, с. 76].

Круг вопросов, подлежащих выяснению у обвиняемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

– при допросе подозреваемого (обвиняемого) в совершении создания вредоносных программ для ЭВМ требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

– при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе обвиняемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ЭВМ, их системы или сети и несанкционированным уничтожением, блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

– на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;

– могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Время нарушения правил можно установить путем допроса свидетелей из числа лиц, участвующих в эксплуатации ЭВМ. При этом могут быть заданы такие вопросы: «Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил (порядка) эксплуатации ЭВМ?». «Когда могло быть нарушено определенное правило эксплуатации ЭВМ, после которого наступили известные вредные последствия?».

Следственный эксперимент.

На последующем этапе расследования преступлений в сфере высоких информационных технологий в целях проверки и иллюстрации собранных по делу доказательств, проверки и оценки следственных версий, установления причин и условий, способствовавших совершению преступления, получения новых доказательств возникает необходимость проведения следственного эксперимента [166; 167; 168; 169]. Как и другие следственные действия, проводящиеся при расследовании преступлений данной категории, следственный эксперимент имеет ряд специфических особенностей, определяющих его виды и специфику тактики.

Виды [166, с. 34; 170, с. 223] следственного эксперимента, проводимого при расследовании неправомерного доступа к компьютерной информации, варьируются и зависят, прежде всего, от способов совершения преступления (непосредственный или опосредованный доступ). В практике при расследовании анализируемого преступления проводятся эксперименты по:

– проверке возможности проникновения в помещение (через двери, окно, с отключением и без отключения сигнализации);

– проверке возможности подключения компьютерной техники и совершения непосредственного доступа к компьютерной информации;

– проверке возможности проникновения в закрытые зоны (путем подбора паролей, идентификационных кодов и установлению периода времени для данного подбора);

– проверке возможности подключения к компьютерной сети;

– проверке возможности электромагнитного перехвата;

– установлению периода времени, необходимого на подключение к компьютерной сети;

– установлению периода времени, необходимого на отключение технических средств защиты информации;

– установлению промежутка времени, необходимого для модификации, копирования компьютерной информации;

– проверке возможности совершения определенных операций к компьютерной информации в одиночку;

– проверке возможности совершения определенных операций с помощью конкретной компьютерной техники за определенный промежуток времени и др.

При проведении следственного эксперимента должны соблюдаться общетактические положения [138, с. 136-151; 167, с. 3-20]:

– оптимальное ограничение количества участников следственного эксперимента;

– максимальное сходство условий проведения следственного эксперимента с условиями, в которых происходило совершение преступления;

– многократность проведения однородных опытов;

– проведение опытных действий в изменяющихся по степени сложности условиях;

– соответствие профессиональных навыков лица, осуществляющего опыты, профессиональным навыкам непосредственного участника исследуемого события;

– обеспечение безопасности участников следственного действия.

При расследовании преступлений в сфере высоких информационных технологий тактические требования приобретают определенные особенности, на которых следует остановиться подробнее.

1. Оптимальное ограничение количества участников следственного эксперимента. Законодательная регламентация круга участников следственного эксперимента позволяет говорить об обязательных и необязательных — в процессуальном смысле слова — участниках этого следственного действия [166, с. 36]. К числу обязательных участников относятся следователь или оперативный работник, которому поручено производство этого следственного действия, и понятые в количестве на менее двух. Как уже отмечалось, понятых следует приглашать из числа лиц, владеющих компьютерной техникой. К числу необязательных участников закон относит подозреваемого, обвиняемого, свидетеля, специалиста, переводчика, педагога, защитника.

Представляется, что присутствие специалиста в области компьютерной техники всякий раз необходимо при проведении рассматриваемого следственного действия по данной категории дел. В целях фиксации показаний с использованием видеосъемки, необходим специалист-оператор. В определенных случаях, необходимо также участие специалиста-криминалиста [171; 172].

Число участников следственного действия должно ограничиваться таким составом (при условии соблюдения уголовно-процессуального законодательства), без которого невозможно получить объективные результаты. Следует иметь в виду, что большое количество участников затрудняет проведение эксперимента, приводит к разглашению его результатов.

2. Максимальное сходство условий проведения следственного эксперимента с условиями, в которых происходило совершение преступления [173; 174]. Обозначенное положение обеспечивается:

а) реконструкцией обстановки для производства опытов, т. е. расположением предметов на месте производства эксперимента в том количестве и порядке,

в каком они находились в момент совершения неправомерного доступа к компьютерной информации. Это позволяет достичь максимального сходства между опытной и реальной обстановкой совершения преступления. Данное требование особенно важно при проверке возможности непосредственного доступа к компьютерной информации, связанного с проникновением преступника в помещение, где установлены средства компьютерной техники;

б) использованием подлинных или сходных по техническим характеристикам (аналогичных) предметов компьютерной техники, программно- и технически совместимого периферийного оборудования, тех же версий программного обеспечения и т. п., о которых говорил обвиняемый;

в) учетом изменившихся и не поддающихся реконструкции условий;

г) воспроизведением (моделированием) субъективных, психофизиологических факторов [175, с. 208].

Как показывает зарубежная практика, внешние условия обстановки при совершении неправомерного доступа к компьютерной информации чаще всего не оказывают такого принципиального значения, как при совершении других преступлений (против собственности, против безопасности дорожного движения и др.). Поэтому при оценке результатов следственного действия необходимо учитывать в первую очередь степень совпадения и соответствия технических характеристик и параметров используемой компьютерной техники, состояния и версий программного обеспечения, типа операционной системы, общей конфигурации компьютера и пр. В то же время, погодные условия (дождь, снег, ветер и пр.) оказывают влияние на результаты опытов по проверке возможности осуществления перехвата информации. К примеру, сильный ветер влияет на распространение электромагнитных волн, создает помехи, препятствует устойчивому приему и др.

Так, если необходимо проверить возможность подключения к компьютерной сети банковского учреждения, состоявшейся в 11 часов, то следователю следует выяснить: сколько компьютеров и в каком режиме работали в это время в данном учреждении; какова в это время загруженность телефонной сети; сколько абонентов одновременно подключалось к данной сети и др. Только после этого провести эксперимент в то же время и в тех же условиях.

При подготовке и проведении следственного эксперимента по проверке возможности электромагнитного перехвата компьютерной информации, распознавания перехваченной информации необходимо участников следственного действия разделить на две группы, в каждой из которых должно быть не менее двух понятых. Первая группа в составе следователя, лица, чьи показания проверяются, понятых, специалиста по средствам компьютерной техники и специалиста, осуществляющего фотосъемку или видеозапись, располагается в том помещении, из которого в свое время осуществлялся перехват.

Вторая группа, включающая оперативного работника, специалиста-криминалиста, понятых и лица, которое будет обрабатывать заранее согласованную со следователем и специалистом компьютерную информацию, размещается в помещении, где находится компьютерная техника. Руководители обе-

их групп перед опытом сверяют часы и обусловливают время начала и продолжительность проведения опытов. Информация выводится на экран неоднократно и в различной последовательности. После окончания опытов обе группы собираются вместе. Следователь оглашает полученные результаты и составляет протокол. В данном случае следственный эксперимент желательно проводить при таких же погодных и климатических условиях, а противном случае они могут повлиять на ход и результаты опытов.

Рассматриваемое следственное действие проводится в том же темпе и при той же продолжительности действий. Например, для проверки возможности копирования определенной информации за конкретный промежуток времени опытные действия необходимо проводить в том же темпе, который имел место при совершении преступления. При этом учитывается также и последовательность действий, составляющих содержание опыта. Например, при определении времени подключения к компьютерной сети, опытные действия должны проводиться в той же последовательности, как об этом говорили обвиняемые на допросе, без предварительной подготовки (включения компьютера, загрузки операционной системы, подключения периферийного оборудования и пр.).

3. Многократность проведения однородных опытов. В целях исключения случайных результатов, обеспечения достоверности и наглядности, опытные действия необходимо осуществлять неоднократно. Количество повторений определяется в зависимости от наступления стабильных, закономерных результатов, при этом не имеет значения, положительный или отрицательный результат будет получен.

4. Изменение условий проведения опытов. В тех случаях, когда следствие не располагает точными данными об условиях, каких-либо параметрах проверяемого события (например, длительность пребывания в компьютерной сети), то необходимо изменять условия проведения опытных действий. Следует иметь в виду, что опытные действия в измененных условиях также повторяются многократно.

Иногда опытные действия целесообразно проводить в измененных условиях, худших по сравнению с теми, что существовали на момент проверяемого события. Такие опытные действия проводятся после экспериментальных, осуществленных в условиях, максимально сходных с теми, что существовали на момент проверяемого события, результаты таких действий усиливают достоверность первых опытных действий.

Если непосредственный участник исследуемых событий не может принять участие в следственном эксперименте, то лицо, заменяющее его, должно подбираться из числа обладающих такими же профессиональными навыками.

5. Обеспечение безопасности участников следственного действия. Всякий раз, принимая решение о проведении следственного эксперимента, следователь должен обеспечить безопасность всех участвующих. Если есть информация о том, что обвиняемый или люди из его окружения могут оказать противодействие проведению эксперимента, расправиться с участниками следственно-оперативной группы, устранить свидетелей [176, с. 15], то необходимо подго-

товить и проинструктировать соответствующим образом подготовленный личный состав следственной группы, предусмотреть применение средств защиты, оружия, специальных средств [177, с. 16].

На процессуальном уровне [178] обеспечение реальной безопасности связано с реализацией требований о неразглашении данных предварительного следствия. Исходя из них, следователь предупреждает понятых, специалиста, переводчика и других лиц, присутствующих при производстве следственного действия, о недопустимости разглашения без его разрешения данных, полученных в процессе опытов.

Тактические рекомендации конкретизируются в зависимости от обстоятельств совершения неправомерного доступа к компьютерной информации (совершенного группой лиц по предварительному сговору, организованной группой), особенностей личностных свойств проверяемого лица, позиции других лиц, проходящих по делу и т. п. К числу наиболее распространенных рекомендаций можно отнести:

– удаление с места проведения следственного действия посторонних граждан;

– проведение следственного действия в такое время, когда исключено присутствие на этом месте посторонних лиц;

– обеспечение охраны (и не только лица, чьи показания проверяются);

– обеспечение оцепления места проведения проверки показаний;

– сокрытие от посторонних данных лица, чьи показания проверяются, и фабулы дела;

– обеспечение приглашения участников следственного действия таким образом, чтобы исключалось их знакомство с лицом, чьи показания проверяются;

– наличие резерва сил для быстрого и эффективного реагирования на экстремальную ситуацию, которая может сложиться при проведении следственного действия и т. п.

Принимая решение о производстве следственного эксперимента, следователь обязан тщательно продумать ход его проведения, комплекс подготовительных мероприятий. Особое внимание необходимо уделить сохранности программного обеспечения и иной компьютерной информации, которая может являться доказательством по делу. Комплекс подготовительных мероприятий, как правило, осуществляется в два этапа: до выезда (выхода) на место проведения следственного эксперимента и по прибытии на него [166, с. 42].

К подготовительным мероприятиям до выезда на место проведения следственного эксперимента относятся:

– изучение и анализ материалов уголовного дела, а в необходимых случаях — ознакомление с оперативно-розыскными данными;

– установление характера и содержания опытных действий; определение места, времени, последовательности проведения опытных действий;

– предварительный выезд (в необходимых случаях) на место проведения следственного эксперимента;

– подготовка средств компьютерной техники, оборудования, программного обеспечения, вещественных доказательств, предметов, которые необходимы для осуществления;

– предупреждение руководителя соответствующего предприятия, организации, учреждения, фирмы или компании, откуда произошел неправомерный доступ к компьютерной информации;

– определение круга участников и принятие соответствующих мер по обеспечению их явки на место производства следственного эксперимента;

– продумывание мероприятий, обеспечивающих охрану места проведения следственного действия;

– подготовка транспортных средств;

– подготовка научно-технических средств и средств связи;

– продумывание мероприятий, обеспечивающих безопасность участников следственного эксперимента.

К подготовительным мероприятиям, осуществляемым по прибытии на место проведения следственного эксперимента, относятся:

– осмотр места опытных действий, принятие мер по реконструкции обстановки (в случае ее нарушения);

– определение места нахождения участников эксперимента, разъяснение способов и средств связи между ними;

– фотографирование обстановки до реконструкции и после нее;

– приглашение понятых, специалистов или других необходимых участников, если это не было сделано заранее;

– разъяснение каждому участнику прав и обязанностей, предупреждение о неразглашении данных эксперимента;

– организация охраны места проведения эксперимента;

– осуществление мероприятий, направленных на реальное обеспечение безопасности участников следственного действия;

– расположение участников в соответствии с планом проведения эксперимента.

Приведенные рекомендации по подготовке к производству следственного эксперимента при расследовании преступлений в сфере высоких информационных технологий носят общий характер и, в зависимости от конкретно эксперимента, должны уточняться. Так, например, очевидно, что при проверке экспериментальным путем возможности перехвата информации на определенном расстоянии важную роль играет выяснение метеоусловий. При подготовке к производству эксперимента по установлению возможности совершить непосредственный доступ к компьютерной информации, эти условия могут не иметь никакого значения и не требовать их выяснения. Что касается тактических особенностей проведения следственного эксперимента, то они также варьируются в зависимости от вида и целей следственного эксперимента.

Предъявление для опознания, наряду с другими следственными действиями, имеет существенное значение для установления и уточнения конкретных

обстоятельств совершенного преступления в сфере высоких информационных технологий. Предъявление для опознания компьютерной информации, предметов и объектов (орудий преступления, магнитных носителей информации и т. п.) позволяет установить не только сами орудия преступления, но и лиц, которые принимали участие в их изготовлении (особенно, при опосредованном доступе), видели их у преступников или изготовителей, определить принадлежность компьютерной информации определенным лицам.

При расследовании рассматриваемой группы преступлений для опознания помимо традиционных объектов (предметы, люди, реже объекты, запечатленные на фотографиях) [179, с. 17] может предъявляться также компьютерная информация в виде программ, баз данных, текстовых или графических файлов, ее носители, компьютерная техника. При этом опознание имеет ряд особенностей, обусловленных спецификой компьютерной информации, рассмотренной нами выше. Предъявление для опознания живых лиц, компьютерной техники и носителей компьютерной информации (как материальных предметов), иных предметов или их фотоизображений [180, с. 161] на практике затруднений не вызывает [138; 179; 181; 182].

Что касается предъявления для опознания компьютерной информации, то здесь имеется ряд сложностей тактического и процессуального характера. Процессуальные сложности связаны с тем, что действующее уголовно-процессуальное законодательство предусматривает в качестве опознаваемых объектов только живых лиц, трупы и предметы. Компьютерная же информация, как и любая информация вообще, сама по себе не материальна. Материальным объектом (предметом) выступает лишь ее носитель. Таким образом, законодательством она не предусматривается как объект предъявления для опознания. Очевидно, это связано с тем, что информация в «чистом виде» не обладает теми идентификационными признаками, которые присущи ее носителю.

Однако, поскольку компьютерная информация все же имеет определенные характеризующие ее идентификационные признаки, такие, как ее содержание, вид, атрибуты, носители, имена и размер файлов, даты и время их создания и т. п., то это, на наш взгляд, делает возможным ее опознание, то есть отождествление. Кроме того, компьютерная информация может обладать и частными индивидуальными особенностями. Так, текст, набранный на компьютере, может иметь различный шрифт, кегль (высота букв), интерлиньяж (расстояние между строк), величину абзацных отступов, особый стиль выделения заголовков, размер полей, особенности нумерации страниц, и т. п.; комплекс признаков конкретного программного продукта: назначение, выполняемые функции, интерфейс, графическое и музыкальное оформление, что делает его пригодным для опознания.

Криминалистические сложности связаны с отсутствием в отечественной литературе методических рекомендаций предъявления для опознания компьютерной информации. Очевидно, в связи с этим, при изучении уголовных дел нам не встретилось ни одного случая предъявления для опознания компьютерной информации. Сложилась практика, когда в некоторых ситуациях необхо-

димо произвести опознание информации (например, обнаруженной и изъятой из ЭВМ в ходе обыска у подозреваемого), следователи производили допрос свидетеля (потерпевшего), в ходе которого демонстрировалась (предъявлялась) данная информация, и допрашиваемое лицо «узнавало» ее в ходе допроса. Представляется, что такой подход не совсем верен, поскольку подобное предъявление уже само по себе может предопределить ответ допрашиваемого лица. На наш взгляд, в подобных случаях необходимо проведение предъявления для опознания.

Перед началом предъявления для опознания опознающий, в соответствии с процессуальным законодательством, должен быть допрошен об обстоятельствах, при которых он видел данную информацию и по каким признакам он сможет провести ее опознание. В процессе допроса необходимо выяснить:

а) объективные факторы наблюдения: знаком ли опознающий с принципами работы ЭВМ; имеются ли у него соответствующие навыки работы на ней; в каких условиях опознающий видел данную информацию, в связи с чем это происходило; как долго происходило наблюдение; на каком компьютере наблюдалась информация (тип процессора, объем оперативной памяти и жесткого диска, применявшееся программное обеспечение и пр.) и т. п.;

б) субъективные факторы, влияющие на полноту и правильность восприятия: состояние зрения (слуха) опознающего; свойства его памяти; хорошо ли он запомнил наблюдаемую информацию; каково ее содержание; каково наименование файла, примерный размер, тип, вид, дата создания, атрибуты;

в) наличие характерных индивидуальных особенностей;

г) может ли опознающий опознать данную информацию в числе однородной.

Довольно серьезную сложность может вызвать процесс предъявления для опознания различного рода программных продуктов, баз данных, текстовых, графических файлов и файлов данных. Закон требует, чтобы предъявление для опознания проводилось в группе однородных предметов. В связи с этим, при подготовке к предъявлению для опознания на основании признаков, указанных опознающим при допросе, подбирается ряд визуально сходных программных продуктов в количестве не менее трех. При заявлении опознающего об опознании программного продукта, его выполнение прекращается и ему предлагается сообщить, по каким именно признакам произошло опознание.

При проведении опознания компьютерной информации не обязательно использовать несколько ЭВМ. Так, в системе WINDOWS возможно параллельное выполнение нескольких программ (просмотр нескольких текстовых или графических файлов, содержимого баз данных) с одновременным выводом результатов на экран. При этом выполнение каждой программы происходит в отдельном окне, размер которого можно увеличить или уменьшить по желанию опознающего. Так же программные продукты, базы данных, тексты и иные файлы можно запускать на одной ЭВМ по очереди, подробно фиксируя последовательность запуска в протоколе. Вопрос о предъявлении для опознании при по-

мощи ЭВМ рассматривался в литературе. Данный прием предлагался при организации опознания вещей [180, с. 87].

В связи с изложенным, полагаем необходимым закрепление в УПК РК положений, регламентирующих использование программных средств при производстве следственных действий, с целью установления доказательственного значения, полученных в ходе их применения, результатов.

Предлагается, дополнить ч. 11 ст. 126 УПК РК «Закрепление доказательств» после слов «киносъемка, фотосъемка» словами «программные средства, использующих технологию оперирования информацией» далее по тексту; после слов «с приведением технических характеристик использованных научно-технических средств» словами «при применении программных средств, использующих технологию оперирования информацией, в протоколе указываются: наименование продукта, версия, код продукта, операционная система, в которой используется программное средство».

Как и в других следственных действиях, при предъявлении для опознания компьютерной информации, желательно участие специалиста и сведущих в компьютерной технике понятых.

В практике могут встретиться случаи, когда на опознающих оказывается воздействие (физическое, психологическое, либо получение денежного или материального вознаграждения) окружением преступников, в связи с чем могут иметь место ложные опознания предъявленных предметов или преднамеренно ложные заявления опознающего о том, что он не опознает предъявленные ему объекты. Поэтому результаты такого опознания подлежат обязательной проверке. Одним из способов проверки является предъявление для опознания тех же предметов другим свидетелям.

В силу различных обстоятельств, при расследовании указанных преступлений, опознающему не всегда могут быть предъявлены для непосредственного опознания: человек, средство компьютерной техники или иной материальный объект в натуральном виде. В этом случае опознание может быть произведено по их фотоснимкам, а иногда и по видеозаписям. Опознание по фотографическим снимкам проводится с соблюдением тех же процессуальных правил и криминалистических рекомендаций, что и опознание в натуральном виде.

Назначение экспертиз.

В зависимости от стоящих перед следствием задач и спецификой объектов исследования для установления конструктивных особенностей и состояния компьютеров, периферийных устройств, магнитных носителей, компьютерных сетей, причин возникновения сбоев в работе указанного оборудования, а также изучения информации, хранящейся в компьютере и на магнитных носителях назначается судебно-технологическая (компьютерная) экспертиза [183], которая представляет собой новый вид судебный экспертизы, необходимость которой обуславливается широким внедрением компьютерной техники и технологий практически во все сферы человеческой деятельности.

В настоящее время в рамках этого рода экспертиз выделяются два вида:

– техническая экспертиза компьютеров и их комплектующих, которая проводится в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей и пр., компьютерных сетей, а также причин возникновения сбоев в работе вышеуказанного оборудования;

– экспертиза данных и программного обеспечения, осуществляемая в целях изучения информации, хранящейся в компьютере и на магнитных носителях.

Положения, касающиеся предмета, объектов, метода исследования и перечня, ставящихся перед экспертом вопросов, достаточно полно исследованы и освещены в научной литературе [11; 23; 184; 185], поэтому мы не будем останавливаться на исследовании данных аспектов.

В настоящей работе мы отразим особенности составления постановления о назначении экспертизы. Отметим, что данное постановление должно содержать максимально полную описательную часть, в которой следует отразить:

– обстоятельства уголовного дела;

– сведения о лицах, причастных к совершению преступления;

– документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование;

– сведения, которые могут быть использованы в качестве «ключевых» слов при восстановлении и(или) поиске экспертом информации (например, названия фирм, учреждений и организаций, фамилии клиентов, предполагаемые номера счетов и т. д.).

В резолютивной части объем задания эксперту должен быть определен конкретно. Современные СВТ имеют большие объемы постоянной памяти в виде жестких дисков (до нескольких гигабайт), поэтому следователь физически не сможет изучить и оценить содержание всего машинного носителя в течение приемлемого для этого времени. Для оптимизации данного процесса темы интересующей следователя информации должны быть точно обозначены при постановке вопросов, а сами они — сформулированы кратко и информативно.

При назначении экспертизы следователь должен четко представлять ее возможности и ограничения, не ставить перед экспертами вопросы и задания, выходящие за рамки их компетенции.

Учитывая специфичность исследования, для разрешения ряда вопросов, возможно совмещение судебно-технической экспертизы с другими. Например, с автороведческой, электроакустической, фоноскопической, видеофоноскопической, радиотехнической, электротехнической и иными техническими экспертизами; в зависимости от отрасли хозяйства или характера нарушений — товароведческие, финансово-экономические, криминалистические, в частности, технико-криминалистические экспертизы документов, созданных с использованием СВТ и новых репрографических технологий, и т. д. [76, с. 147].

ЗАКЛЮЧЕНИЕ

В работе на основе исследования и анализа нормативного, теоретического и эмпирического материала были освещены проблемы законодательной регламентации и практической реализации процессуального порядка получения и использования информации с технических каналов связи в уголовном судопроизводстве, сформулированы конкретные выводы и предложения.

1. Определена специфика компьютерной информации, заключающаяся в следующем:

1) данная информация, как правило, очень объемна и быстро обрабатываема;

2) эта информация очень легко и, как правило, бесследно уничтожаема;

3) компьютерная информация обезличена, т. е. между ней и лицом, которому она принадлежит, нет жесткой связи;

4) данный вид информации может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и др.), в самой ЭВМ (оперативной памяти — ОЗУ);

5) рассматриваемый вид информации может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВТ при наличии соответствующих периферийных устройств чтения машинных носителей информации (дисководы, устройства чтения лазерных дисков (CD-ROM), стримеры, устройства чтения цифровых видеодисков и др.);

6) эта информация легко передается по телекоммуникационным каналам связи компьютерных сетей, причем практически любой объем информации можно передать на любое расстояние.

2. Определена классификация компьютерной информации по:

– ее носителям — зафиксированная на магнитной ленте, дискетах (Floppy Disk), лазерных дисках, на жестком диске ЭВМ (Hard Disk), в памяти ЭВМ, системы ЭВМ или сети;

– типу — текстовая, числовая, графическая и др.;

– местонахождению;

– наименованию файла — символьное описание названия;

– размеру (объему) — количество страниц, абзацев, строк, слов, символов или байт;

– времени создания, времени изменения;

– атрибутам (архивная, скрытая, системная, только для чтения и др.).

При этом факультативными свойствами могут быть: тема, автор, создавший или изменивший информацию, группа, в которую включен данный файл, ключевые слова, заметки автора или редактора.

3. Разработано определение понятия «преступления в сфере высоких информационных технологий», под которыми понимается совершение противоправных деяний в области информационных отношений, осуществляемых посредством высокоточного оборудования, устройств и программных средств,

использующих технологию оперирования информацией. Данный термин наиболее точно определяет преступления в рассматриваемой нами области. Расследование преступлений, совершенных с использованием средств компьютерных технологий, в таком случае будет являться составной частью расследования преступлений в сфере высоких информационных технологий.

Следует отметить следующие характерные особенности преступления в сфере высоких информационных технологий:

– неоднородность объекта посягательства;

– выступление компьютерной информации, как в качестве объекта, так и в качестве средства преступления;

– многообразие предметов и средств преступного посягательства;

– выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

4. Учитывая, что использование высокоточного оборудования и устройств, использующих технологию оперирования информацией, при совершении различного вида преступлений, свидетельствует о повышенной общественной опасности таких действий, а также то, что уголовно-правовое законодательство не в состоянии оперативно квалифицировать стремительное развитие всех видов и способов совершения указанной категории преступлений предлагается дополнить ч. 1 ст. 54 УК РК «Обстоятельства, отягчающие уголовную ответственность и наказание», п. «р», изложив его в следующей редакции: «р) совершение преступления с использованием высокоточного оборудования, устройств и программных средств, использующих технологию оперирования информацией».

Классификацию преступлений в сфере высоких информационных технологий следует осуществлять по следующим критериям:

– высокоточное оборудование, устройства и программные средства, использующие технологию оперирования информацией, компьютерная информация, являются объектом правонарушения;

– высокоточное оборудование, устройства и программные средства, использующие технологию оперирования информацией, компьютерная информация, используются как орудия и средства, способствующие совершению преступления.

Предложенная классификация позволит систематизировать уголовно-правовые аспекты определения видов преступлений в сфере высоких информационных технологий, а также определить способы совершения, конкретные приемы их применения, используемые при этом технические средства, методы подготовки и исполнения преступления и множество иных обстоятельств, имеющих следственно-оперативное значение при расследовании и раскрытии преступлений в сфере высоких информационных технологий.

5. Раскрывая криминалистическую характеристику преступлений в сфере высоких информационных технологий, определена классификация способов совершения преступлений в сфере высоких информационных технологий и

рассмотрено их содержание. Способы совершения объединены в три основные группы:

1) несанкционированный доступ к средствам компьютерной техники, к которому относятся действия преступника, направленные на: изъятие средств компьютерной техники, информации; получение несанкционированного доступа к средствам компьютерной техники, к компьютерным системам, компьютерной информации;

2) манипуляция данными и управляющими командами — действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники в целях осуществления подмены входных и выходных данных в процессе автоматизированной обработки документов или внесение умышленного изменения в существующую программу, заведомо приводящего к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т. д.;

3) комплексные методы, под которыми понимаются использование преступником двух и более способов, а также их различных комбинаций при совершении преступления.

Исследованы особенности следов преступлений в сфере высоких информационных технологий, которые классифицированы на два типа: традиционные следы (следы-отображения, рассматриваемые трасологией, а также следы-вещества и следы-предметы) и нетрадиционные — информационные следы (отражают изменения в хранящейся в них информации по сравнению с исходным состоянием). Дано графическое отображение следовой картины, включающей:

а) следы на машинных носителях, посредством которых действовал преступник на своем рабочем месте и возле машинных носителей, принадлежащих преступнику;

б) следы на «транзитных» (коммуникационных) машинных носителях, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися нападению;

в) следы на машинных носителях информационной системы, в которую осуществлен неправомерный доступ.

6. В ходе исследования определено, что смешение понятий орудия и средства совершения преступлений ведет к непомерному расширению объема понятий орудий преступления, так и функциональному назначению охватываемых ими предметов. С учетом изложенного, орудиями совершения преступлений в сфере высоких технологий являются: компьютер и технические средства, используемые непосредственно для незаконного получения сведений; а средствами совершения преступлений в сфере высоких информационных технологий являются: сетевое оборудование, телефонная сеть, телефон, телевизионный кабель, компьютерные системы, контрольно-измерительная аппаратура, устройства для регистрации электромагнитного излучения, специальное программное

обеспечение, периферийное оборудование, а также носители компьютерной информации и т. д.

7. Наиболее важным компонентом обстановки подготовки, исполнения и сокрытия преступления в сфере высоких информационных технологий являются специфические условия деятельности потерпевших сторон, которые разграничиваются на объективные и субъективные.

8. Местом совершения преступлений в сфере высоких информационных технологий являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в каком-либо технологическом процессе. Особенностью совершения преступлений в сфере высоких информационных технологий является то, что место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать. Из изложенного следует, что преступления в сфере высоких информационных технологий имеют транснациональный характер — преступление совершается в одной стране, а негативные последствия наступают в другой.

9. Определена классификация видов субъектов преступлений в сфере высоких информационных технологий. К первой группе относятся лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей. Вторая группа — лица, страдающие новым видом психических заболеваний — информационными болезнями или компьютерными фобиями. Изучением этих болезней в настоящее время занимается новая, сравнительно молодая отрасль медицины — информационная медицина. Преступления, совершаемые преступниками данной группы, в основном связаны с физическим уничтожением либо повреждением средств компьютерной техники без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями. Третью группу составляют профессиональные преступники, с ярко выраженными корыстными целями. Они характеризуются многократностью совершения преступлений с обязательным использованием действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми преступными навыками. Это высококвалифицированные специалисты, имеющие высшее техническое образование.

По категориям доступа к средствам компьютерной техники субъектов преступлений в сфере высоких информационных технологий можно разделить на две подгруппы:

– внутренние пользователи (лица, которые имеют непосредственный доступ к необходимой информации);

– внешние пользователи (субъекты, которые обращаются к информационной системе или посреднику за получением необходимой им информации).

На основе проведенного анализа возраста, образования, мотивации совершения преступления, даны основные характеризующие признаки преступников. В целом, следует отметить, что возраст преступников колеблется от 15 до 45 лет, на момент совершения преступления возраст у 33 % преступников не превышал 20 лет, 13 % — старше 40 лет и 54 % — 20-40 лет.

10. Наиболее распространенными мотивами совершения преступлений в сфере высоких информационных технологий являются: 1) корыстные соображения — 66 % (совершаются в основном преступниками третьей группы); 2) политические цели — 17 % (шпионаж, например, совершается преступниками третьей группы); 3) исследовательский интерес — 7 % (студенты и профессиональные программисты первой группы); 4) хулиганские побуждения и озорство — 5 % (хакеры, преступники первой группы); 5) месть — 5 % (преступники первой и второй групп).

Наиболее типичными преступными целями совершения преступлений в сфере высоких информационных технологий являются: 52 % — хищение денежных средств; 16 % — разрушение и уничтожение средств компьютерной техники; 12 % — подмена исходных данных; 10 % — хищение информации и программ и 10 % — хищение услуг.

11. Определен перечень основных обстоятельств (17 позиций), подлежащих доказыванию и установлению по делам о преступлениях в сфере высоких информационных технологий, с учетом особенностей данной категории деяний, находящихся на стыке права и технологии.

12. По делам рассматриваемой категории выделены типичные исходные следственные ситуации: 1) информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует; 2) имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника; 3) известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

По каждой ситуации определены программы проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий.

В соответствии с вышеуказанными программами предложен перечень общих и частных следственных версий.

13. Разработаны методические рекомендации и схемы расследования первоначального этапа расследования отдельных видов преступлений в сфере высоких информационных технологий — при расследовании: неправомерного доступа к охраняемой законом компьютерной информации; создания, использования и распространения вредоносных программ для ЭВМ; преступления, совершенного в условиях неочевидности; нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.

14. Исследованы тактические особенности проведения отдельных следственных действий при расследовании преступлений в сфере высоких информационных технологий: осмотра (места происшествия, средств вычислительной техники, машинного носителя информации, машинного документа), обыска, выемки, допроса (подозреваемого, обвиняемого, свидетелей), следственного эксперимента, предъявления для опознания, назначение экспертиз.

Определен и раскрыт перечень мероприятий на подготовительном этапе (планирование, состав следственно-оперативной группы (инструктаж группы), особенности состава и выбора участников, обеспечение безопасности участников следственного действия, подготовка соответствующей компьютерной техники и программного обеспечения и т. д.); перечень действий при непосредственном производстве следственного действия (общетактические положения, тактические рекомендации по особенностям проведения действия, применения компьютерной техники и программного обеспечения, перечень наиболее значимых моментов, подлежащих обязательному исследованию, перечень тактических приемов, рекомендации по принятию действий в целях недопущения вредных последствий перечня факторов, направленных на срыв следственного действия или уничтожения доказательств преступного деяния и др.); необходимость соблюдения рекомендаций по специфике изъятия, хранения, транспортировке изъятого, особенностям составления, оформления процессуальных документов и т. д. на заключительном этапе.

15. С целью установления доказательственного значения результатов, полученных в ходе применения программных средств при производстве следственных действий, предлагается дополнить ч. 11 ст. 126 УПК РК «Закрепление доказательств» после слов «киносъемка, фотосъемка» словами «программные средства, использующих технологию оперирования информацией» далее по тексту; после слов «с приведением технических характеристик использованных научно-технических средств» словами «при применении программных средств, использующих технологию оперирования информацией, в протоколе указываются: наименование продукта, версия, код продукта, операционная система в которой используется программное средство».

16. Исследовано: современное состояние деятельности органов внутренних Республики Казахстан в борьбе с преступлениями в сфере высоких информационных технологий на примере функционирования «Управления по организации борьбы с преступлениями в сфере информационных технологий Комитета криминальной полиции МВД РК»; осуществление РК оперативного взаимодействия с зарубежными правоохранительными органами по транснациональным преступлениям в сфере высоких технологий. Определены перспективы совершенствования борьбы с преступлениями в сфере высоких информационных технологий.

Кроме указанных выводов следует определить следующие перспективы исследования, вытекающие из проведенной работы:

– определение методики расследования преступлений в сфере высоких информационных технологий на последующем этапе расследования;

– проведение исследований методик расследования отдельных видов преступлений в сфере высоких информационных технологий на основе предлагаемой нами трактовки сущности и содержания тактической комбинации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Назарбаев Н. А. Стратегия вхождения Казахстана в число 50-ти наиболее конкурентных стран мира. Казахстан на пороге нового рывка вперед в своем развитии: Послание Президента РК народу Казахстана // Индустриальная Караганда. 2006. 2 марта.

2 Закон Республики Казахстан №233-1 от 26 июня 1998 года «О национальной безопасности» // Казахстанская правда. 1998. 7 июля.

3 Крылов В.В. Информация как элемент криминальной деятельности // Вестник Моск. ун-та. Сер. 11. Право. - М., 1998.-№4.-С.50-64.

4 Дулов А.В. Криминалистический анализ компьютерных преступлений. // Проблемы "компьютерной преступности": Выпуск 2. — Мн.: НИИ ПККСЭ МЮ РБ, 1992. С.1.

5 Селиванов Н.А. Проблемы борьбы с компьютерной преступностью. // Законность. — М., 1993, №8. С.37.

6 Крылов В.В. Расследование преступлений в сфере информации. М.. 1998. С. 2.

7 Батурин Ю.М. "Компьютерное преступление" — что за термином? // Право и информатика. - М.: МГУ, 1990. С.9.

8 Ахраменка Н.Ф. Криминализация общественно опасного поведения с использованием информационно-вычислительных систем. С.23.

9 Курушип В.Д., Минаев В,А. Компьютерные преступления и информационная безопасность. М., 1998

10 Ляпунов Ю.И., Максимов С.В. Ответственность за компьютерные преступления// Законность. 1997. № 1;

11 Россинская Е.Р., Усов АМ. Судебная компьютерно-техническая экспертиза. М., 2001. С. 21

12 International review of criminal policy - United Nations Manual on the prevention and control of computer related crime // http://conventions.coe.int/treaty/en/projets/ cybercrime.htm.

13 Marc D. Goodman. Why the Police Don't Care About Computer Crime, 10 Harvard Journal of Law & Technology 465, 468-469 (1997).

14 Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995. С. 71.

15 Проблемы преступности за рубежом: Реферативный обзор. — М.: ГИЦ МВД СССР, 1988. С.18

16 ; Законодательство о борьбе с компьютерными преступлениями. // Проблемы преступности в капиталистических странах. — М.: ВИНИТИ, 1989, №1. С.8.

17 Горбатов В.С., Полянская О.Ю. Мировая практика криминализации компьютерных правонарушений. М, 1998.

18 Компьютерная преступность в Великобритании. // Проблемы преступности в капиталистических странах. — М.: ВИНИТИ, 1990, №8. С.14.

19 Проблемы преступности в капиталистических странах. — М.: ВИНИТИ, 1987. №2. С.13.

20 Компьютерное проникновение или заговор // Форпост. 2002. 4 июня.

21 Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: Сб. матер. межд. конф. 1 — 2 марта 2001 г. — Алматы: Интернет трейнинг центр, 2001.

22 Юридический энциклопедический словарь / Под ред. А. Я. Сухарева. — М., 1987. — 82 с.

23 Сырбу А. В. Процессуальный порядок получения и использования информации с технических каналов связи в уголовном судопроизводстве: Дис. … канд. юрид. наук. — Караганда, 2005. — 191 с. С-45

24 Шурухнов Н.Г., Левченко И.Н., Лучин И.Н. Специфика проведения обыска при изъятии компьютерной информации // Актуальные проблемы совершенствования деятельности ОВД в новых экономических и социальных условиях. М., 1997. С. 208-216.

25 Информация о преступлениях в сфере высоких технологий. — М.: ГИЦ МВД РФ, 1999.

26 Существующие технологии работы с банковскими картами являются уязвимыми для хакеров. Источник: www.vsluh.ru

27 Катаев С.Л. Социальные аспекты компьютерной преступности // Центр иссл. пробл. комп. преступн. — Киев, 2002.

28 Крылов В.В. Информационные компьютерные преступления. — М.: ИНФРА-М-НОРМА, 1997.

29 Анин Б. Защита компьютерной информации. — СПб.: BHV, 2000.

30 Noise around of safety of bank systems // London Times. 1996. 3 June.

31 Оспанов Е.Т. Орудие преступления — компьютер // Бюллетень ГСУ и ЭКУ МВД РК. — Алма-Ата: МВД РК, 1995.- №1-2(1-5).-С.35-41.

32 Уголовный кодекс Республики Беларусь от 9.07.1999. // Ведомости Национального собрания Республики Беларусь, 1999 г., №24, ст.420.

33 Вопросы квалификации и расследования некоторых преступлений в сфере экономики: Материалы семинара (15-18 декабря 1998 г.). Саратов, 1999. С. 166-168

34 Черкасов В.Н. О понятии "Компьютерная преступность". // Проблемы компьютерной преступности: Выпуск 2. — Мн.: НИИ ПККСЭ МЮ РБ, 1992. С.5.

35 Куринов Б.Л. Научные основы квалификации преступлений. М., 1984;

36 Никифоров Е. С. Об объекте преступления по советскому уголовному праву // Сов. государство и право. 1956. №6

37 Кудрявцев В.И. Общая теория квалификации преступлений. М., 1972;

38 Ляпунов Ю.И. Общественная опасность деяния как универсальная кате-

гория советского уголовного права. М., 1990;

39 Динека В.И. Объект преступления // Уголовное право. Общая часть / Под. ред. Н.И. Ветрова, Ю.И. Ляпунова. М., 1997. С. 184.. и др.

40 Ветров Н.И. Уголовное право. М., 1999. С. 183-184.

41 Исаев А.А. Применение специальных познаний для квалификации преступлений. — Алматы: Мектеп, 1997

42 Нугманова А. Т. Частная жизнь граждан под наблюдением высоких технологий // Вестник Университета им. Д. Кунаева. — 2005. — № 2(15). — С. 34-39.

43 Закон Республики Казахстан от 8 мая 2003 года № 412-II Об информатизации (с изменениями, внесенными Законом РК от 20.12.04 г. № 13-III);

44 Постановление Правительства Республики Казахстан от 22 июля 2003 года № 724. Вопросы Агентства Республики Казахстан по информатизации и связи (с изменениями, внесенными постановлениями Правительства РК от 24.11.04 г. № 1232; от 17.05.05 г. № 464)

45 Приказ и.о. Председателя Агентства РК по информатизации и связи от 17 января 2005 года N 10-п "О внесении изменений и дополнений в приказ Председателя Агентства РК по информатизации и связи от 12 июля 2004 года N 145-п "Об утверждении Правил присоединения сетей телекоммуникаций к сети телекоммуникаций общего пользования и регулирования пропуска трафика по сети телекоммуникаций общего пользования РК "

46 Приказ Председателя Агентства РК по информатизации и связи от 31 августа 2004 года № 181-П «О внесении изменений в приказ Председателя Комитета по связи и информатизации Министерства транспорта и коммуникаций РК от 11 марта 2003 года № 13-п «Об утверждении Правил оформления разрешительных документов в области связи и регистрации радиоэлектронных средств и высокочастотных устройств» (зарегистрирован за № 2234)»

47 Совместный приказ председателя КНБ РК от 20 сентября 2004 года № 179 и и. о. председателя Агентства РК по информатизации и связи от 20 сентября 2004 года № 199-п «Об утверждении Правил взаимодействия государственных органов и организаций при внедрении и эксплуатации аппаратно-программных и технических средств проведения оперативно-розыскных мероприятии на сетях телекоммуникаций Республики Казахстан // Реестр государственной регистрации нормативных правовых актов Республики Казахстан 5 ноября 2004 года под № 3187.

48 Нугманова А. Т. Общие требования при реализации ОРМ на сетях телекоммуникаций // Информационно-коммуникационные технологии как основной фактор развития инновационного общества: Мат-лы международ. науч.-практ. конф. — Усть-Каменогорск, 2007. — С. 120-121.

49 Нугманова А. Т. «Перспективные» проблемы организации проведения оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Казахстан // Экономика и право Казахстана. — 2005. — № 11. — С. 48-51.

50 Батурин Ю.М. Проблемы компьютерного права. — М.: Юриздат, 1991. С.31.

51 Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации. // Конфидент. — С-Петербург, 1999, №4-5.

52 Расследование компьютерных преступлений. Вечерский Д.А Шалькевич И.И., Минск 2001с. 13с.

53 Экенвайлер М. "Преступная деятельность, совершаемая с использованием режима "онлайн" (Тезисы докладов на международной конференции "Проблемы борьбы с новыми видами экономических преступлений в России и США", 20-21 мая 1997 года). — Internet: http://www.uic.ssu.samara.ru/~cclub/navigator/uglaw.htm

54 Яблоков Н.П. Исследование обстоятельств преступных нарушений правил безопасности труда. М., 1980. С. 32-33;;;

55 Колесниченко А.Н., Коновалова В.Е. Криминалистическая характеристика преступлений. Харьков, 1985.; и др

56 Джакишев Е.Г. Криминалистическая характеристика преступлений и ее значение в определении основных обстоятельств, подлежащих доказыванию. // Некоторые вопросы борьбы с преступностью в Казахской ССР. Сб. научных трудов. — Алма-Ата, изд-во КазГУ, 1987 С. 231

57 Мозговых Г.А. Криминалистическая характеристика преступления. Алматы, 2001.- 247 с.

58 Мозговых Г.А. Криминалистическая характеристика преступлений и ее значение в методике расследования // Вестник КазГУ, серия юридическая, № 4 (17). — Алматы, 2000 С. 65

59 Эйсман А.А. О содержании понятия криминалистическая характеристика преступления // Криминалистическая характеристика преступлений. — М.: ВНИИ Прокуратуры СССР, 1984, С. 170.

60 Герасимов И.Ф. Криминалистические характеристики преступлений в методике расследования. Методика расследования преступлений / Общие положения: Материалы научно-практической конференции (г.Одесса, ноябрь, 1976), С. 159.

61 Крылов И.В. Криминалистическая характеристика и ее место в системе науки криминалистики и вузовской программе. // Криминалистическая характеристика преступлений. Сб. научных трудов ВНИИ Прокуратуры СССР, 1984. С. 169.

62 Танасевич В.Г., Образцов В.В. О криминалистической характеристике преступлений. // Вопросы борьбы с преступностью. - М., Юридическая литература, 1976. Выпуск 25. С. 193.

63 Васильев А.Н. О криминалистической классификации преступлений. // Методика расследования преступлений. - М., 1976. С 225.

64 Лузгин И.М. Некоторые аспекты криминалистической характеристики и место в ней данных о сокрытии преступлений. // Криминалистическая характеристика преступлений. М., 1984. С. 54.

65 Селиванов Н.А. Криминалистические характеристики преступлений и следственные ситуации в методике расследования. // Социалистическая законность. № 2, 1977, С. 64.

66 Колесниченко А.Н. Теоретические проблемы криминалистической характеристики. // Криминалистическая характеристика преступлений. — М., 1984, С.217.

67 А.Н.Васильев. Н.П. Яблоков / Предмет, система и теоретические основы криминалистики М. 1984 г. С. 215.

68 Криминалистика под ред. И.Ф. Пантелеева, Н.А. Селиванова. — М., 1988. С. 489.

69 Криминалистика Под. Ред. П.Н. Яблокова В.Я.Колдина. — М., 1990 С. 424.

70 Криминалистическая энциклопедия Под.ред Р.С. Белкина - Алматы. 1995. С. 363.

71 Шурухнов Н.Г. Криминалистическая характеристика преступлений. Криминалистика (актуальные проблемы) / Под ред. Е. И. Зуева. М., 1988. С. 119

72 Шурухнов Н.Г. Расследование краж. М., 1999. С. 21.

73 Лавров В.П. Учение о способе преступления. Криминалистическая характеристика преступления // Курс лекций по криминалистике /Под ред. А.Ф.Волынского. Вып. 10. М., 1999. С. 75-91 с.85

74 Белкин Р.С. Курс криминалистики в 3 т. — М. 1997 г. Т.3 С. 389.

75 Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. - М.: ЮИ МВД РФ, 2003. с. 55=- 245 с.

76 Зуйков Г.Г. Поиск преступников по способу совершения преступлений. М, 1970. С. 26;

77 Кустов А.М. Теоретические основы криминалистического учения о механизме преступления М., 1997. С. 107-105;

78 Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. М.: Право и Закон. 1996.

79 Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: Автореф. дисс... канд. юрид. наук. М.,1997. С. 14.

80 Прохоров А.С. Расследование преступлений в сфере компьютерной информации (учебно-методическое пособие)Москва, 1998 год с. 57-58= 120с.

81 Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом. М.: ВИНИТИ, 1992, №4. С.3-10.

82 Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. — Internet: http://www.melik.narod.ru

83 Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. — М.: Горячая линия-Телеком, 2002. — 336 с.

84 Батурин Ю.М., Укодзишский А.М. Компьютерная преступность и компьютерная безопасность. М., 1991. С. 18-34;

85 Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений; Дис.... канд. юрид наук М.,1997. С. 83-101;

86 Родионов А. Н., Кузнецов А.В. Расследование преступлений в области высоких технологий // Вестник МВД России. 1999. № 6. С. 65-70 и др.

87 Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. М., 2001. С. 19-20, 27 с.

88 Эд Тайли. Безопасность компьютера. Минск: “Пепурри”, 1997

89 Архив районного суда г. Павлодара за 2003 г. Уголовное дело по обвинению К. по ст. 227 ч. I УК РК.

90 Сергеев В. В. Компьютерные преступления в банковской сфере // Банковское дело. 1997. № 2. С. 27-28

91 Лучин И.Н., Желдаков А.А., Кузнецов Н.А. Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем. М.: Академия МВД России, 1996. С.287-288.

92 Архив районного суда Уральской области. Уголовное дело № 60/98 по обвинению гр. У. по ст. 227 ч.2 УК РК

93 Michel J. Palmiotto. Criminal investigation. Nelson-Hall publishers. Chicago. 1994. P. 486.

94 Гудков П.Б. Компьютерные преступления в сфере экономики // В сб. Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. М.: МИ МВД России, 1995. 120с.

95 Безруков Н.Н. Компьютерные вирусы. — М.: Наука, 1991. С.100.

96 Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. 1993. №8. 96

97 Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность, 1994. №6. С.44-47.

98 Стив Басс // Мир ПК. — 2002. — № 4. — С. 94-95

99 Архив Казыбекбийского суда г. Караганды. Уголовное дело по обвинению гр. Л. и М. по ч.2 ст. 227 УК РК

100 Архив Алмалинского районного суда г. Алматы за 2004 г.

101 Кошанов У.К. Уголовно-правовое значение орудий и средств совершения преступлений. Автореферат на соиск. Уч.степ. к.ю.н. Караганда 2006 с.15 - 30с.

102 В соответствии с Законом Республики Казахстан «О связи» от 13 мая 1999 г. // Казахстанская правда. 1999. 21 мая. -

103 Куликов В.И. Обстановка совершения преступления и ее криминалистическое значение: Автореф. дис.... канд. юрид. наук. М., 1983. С. 15.

104 Образцов В.А. Криминалистическая классификация преступлений. Красноярск, 1988. С. 99.

105 В.Б. Вехов. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: Учеб.-метод. пос. Изд. 2-е, доп. и испр. - М.: МЦ при ГУК и КП МВД России, 2000. — 64 с.

106 Черных Э., Черных А. «Компьютерные» хищения: как их предотвратить? // Юстиция. 1993. №3. С. 21.

107 Криминалистика / Под ред. Р.С. Белкина. М., 1999, С. 952.

108 Букин Д. Хакеры. О тех, кто делает это//Рынок ценных бумаг. 1997. № 23. с.11

109 Букин Д. Underground киберпространства // Рынок ценных бумаг. 1997. № 18. С. 104-108

110 Крылов В.В. Расследование преступлений в сфере компьютерной информации. Криминалистика / Под ред. Н.П. Яблокова М., 1999. С. 620.

111 Diagnostic and Statistical Manual of Mental Disorders - Fourth Edition «DSM-IV», American Psychiatric Association, 1995

112 Crime in Cyberspace First Draft of International Convention Released for Public Discussion//http://conventions.coe.mt/treaty/en/projets/cybercrime.htm.

113 Минаев В.А., Саблин В.Н. Основные проблемы борьбы с компьютерными преступлениями в России. — Internet: http://www.mte.ru/www/toim.nsf

114 Уголовное право. Общая часть/Под ред. Н.И.Ветрова, Ю.И.Ляпунова М, 1997. С. 239;

115 Волков Б. С. Мотивы преступлений (уголовно-правовое и социально-психологическое исследование). Казань, 1982

116 Панов В.П. Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 1993. С.14.

117 Головин А.Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // http://www.crime-research. org/library/Go Iovin.htm.

118 Уголовно-процессуальный кодекс Республики Казахстан ст. 19 часть 1. Алматы 1998 г. С 353.

119 Малько А.В, Матузов Н.И. «Теория государства и права» М 2001 г. С. 512.

120 Кенжетаев И.Д. Методика расследования посредничества во взяточничестве на первоначальном этапе.: Дис. … канд. юрид. наук. — Караганда, 2006. — 141 с. С-50

121 Ермолович В.Ф. Механизм определения обстоятельств, подлежащих выяснению и доказыванию при расследовании преступлений. // Вопросы криминологии, криминалистики и судебной экспертизы. Выпуск №10. — Мн., 1994. С.81.

122 Лузгин ММ. Методика изучения, оценки и разрешения исходных следственных ситуаций. Исходные следственные ситуации и криминалистические методы их разрешения; Сб. научных трудов. М., 1991. С. 10-21.;

123 Драпкин Л.Я. Общая характеристика следственных ситуаций. Следственная ситуация. М., 1985. С. 13.;

124 Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: Автореф. дис.... д-ра юрид. наук. Харьков, 1967. С. 509, и др.

125 Скоромников К.С. Особенности расследования неправомерного доступа к компьютерной информации. Расследование преступлений повышенной общественной опасности: Пособие для следователя / Под ред. Н.А. Селиванова, А.И. Дворкина. М, 1998. С. 348-349

126 Егоров Г.А., Ващепко В.С., Кузнецов А.В. Учебное уголовное дело: Учебно-практическое пособие. Иркутск, 2000.

127 Архив районного суда г. Усть-Каменогорска за 2001 г.

128 Архив Атырауского городского суда за 2002 г.

129 Архив Бостандыкского районного суда г. Алматы за 2000 г.

130 По материалам следственного управления ДВД г. Шымкент за 2005 г..

131 Сергеев В. В. Компьютерные преступления в банковской сфере // Банковское дело. 1997. № 2. С. 26.

132 Васильев А.Н. Следственная тактика. — М.: Юридическая литература, 1976. С. 324

133 Васильев А.Н. Тактика отдельных следственных действий. — М.: Юридическая литература, 1981. С. 274

134 Дулов А.В., Нестеренко П.Д. Тактика следственных действий. — Минск: Высшая школа, 1971. С. 223

135 Бахарев Н.В. Очная ставка: Уголовно-процессуальные и криминальные вопросы. — Казань: КУ, 1982. С. 183

136 Порубов Н.И. Допрос в советском уголовном судопроизводстве. — Минск, 1973 С. 231

137 Глазырин Ф.В. Психология следственных действий. - Волгоград, 1983 С.346

138 Ратинов А.Р. Судебная психология для следователей. — М., 1967 С. 126.

139 Белкин Р.С. /Курс Советской криминалистики М. 1979 г. Т 3. С. 437

140 Белкин Р.С., Лившиц ЕМ. Тактика следственных действий. М., 1997. Гл. 2.;

141 Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях. СПб., 1998. С. 29-35;

142 Головин А.Ю., Коновалов С.И., Толстухина Т.В. Тактика осмотра и обыска по делам о преступлениях в сфере компьютерной информации: Лекция. Тула, 2002;

143 Назмышев Р. А. Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. С. 15. и др.

144 Винницкий Л.В. Осмотр места происшествия: организация, процессуальные и тактические вопросы. Караганда., 1986. С. 18-36.

145 Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: Дис.... канд. юрид. наук. М., 2000. С. 73;

146 Касаткин А.В. Тактика собираний и использования компьютерной информации при расследовании преступлений: Дис.... канд. юрид. наук. М.,1997. С. 91.

147 Осипенко М. Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. 1994. № 10. С. 16.

148 Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства защиты объектов информации: Справочное пособие. СПб., 1996. С. 149-150.

149 ЗубахаВ.С., УсовА.И., СаенкоГ.В., Волков ГА., Белый С.Л., Семикалепова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. М., 2000. С. 16-21.

150 Катков С.А., Собецкий И.В., Фёдоров А.Л. Подготовка и назначение программно-технической экспертизы // Информ. бюллетень СК МВД России. — 1995. — № 4(85). — С. 92=96с.

151 Постановление Кабинета Министров Республики Казахстан от 30 июня 1992 г. № 562 «Об утверждении Основных правил документирования и управления документацией в объединениях (предприятиях), учреждениях и организациях всех организационно-правовых форм Республики Казахстан» — Алматы, 1992.

152 Закон РК от 7 января 2003 г. № 370-II «Об электронном документе и электронной цифровой подписи» // Каз. правда. 2003. 10 янв.

153 Криминалистика. под ред. А.В. Дулова. — Мн., 1996. С.290, 326.

154 Долгипов С.Д, Использование обыска в раскрытии, расследовании и предотвращении преступлений, М., 1997;

155 Михайлов А.И,,ЮрииЕ.С. Обыск. М., 1971

156 Шурухнов Н.Г., Лучин И.Н. Методические рекомендации по изъятию компьютерной информации при проведении обыска // Информационный бюллетень Следственного комитета МВД РФ. М., 1996. № 4(89). С. 22-28; и др

157 Иванов А.Н. Производство обыска: уголовно процессуальные и криминалистические аспекты / Под ред. В.И. Комиссарова. Саратов, 1999. С. 62

158 Особенности производства обыска при расследовании компьютерных преступлений (М.М. Менжега, "Журнал российского права", N 12, декабрь 2003 г.60с.)

159 Комиссаров В., ГавриловМ., Иванов А. Обыск с извлечением компьютерной и информации // Законность. 1999. № 3.90

160 Крылов В.В. Указ. раб. С. 250-252.; Филиппов А,Г. Тактика допроса и очной ставки: Криминалистика / Под ред. А.Г. Филиппова, А.Ф. Волынского. М., 1998. С. 289-291 и др.

161 Соловьев А.Б. Использование доказательств при допросе. М., 1981. С. 77.

162 КарнееваЛ.М., СтаткусВ.Ф. Предъявление обвинения. М, 1973. С. 120.

163 Кулагин Н.И., Порубов Н.И. Организация и тактика допроса в условиях конфликтной ситуации. Минск, 1977;

164 Ратинов А.Р., Адамов ЮМ. Лжесвидетельство. М., 1977 и др.

165 Казинян Г.С., Соловьев А.Б. Проблемы эффективности следственных действий. Ереван, 1987. С. 76-86.

166 Белкин Р.С., Белкин А.Р. Эксперимент в уголовном судопроизводстве. М., 1997.;

167 Щурухнов Н.Г. Тактика следственного эксперимента. Криминалистика: Курс лекций / Под ред. В.П. Лаврова. Вып. 7. М., 1997. С. 21-44.;

168 Глазырин Ф.В., Крутиков А.П. Следственный эксперимент. Волгоград, 1981.;

169 Жукова Н.И, Жуков А.М. Производство следственного эксперимента. Саратов, 1989.

170 Белкин Р. С. Эксперимент в следственной, судебной и экспертной практике. М., 1964. С. 223.; Белкин Р.С., Белкин А.Р. Эксперимент в уголовном судопроизводстве. М., 1997. С. 34.

171 Астапкина С.М.,ДубровицкаяЛ.П., ПлесовскихЮ.Г. Участие специалиста-криминалиста в расследовании преступлений. М., 1992. С. 55-57;

172 Слепнева Л.И. Взаимодействие следователя ОВД с сотрудниками криминалистических подразделений в процессе раскрытия и расследования преступлений: Дис.... канд. юрид. наук. М., 1987 и др.

173 Куванов В.В. Реконструкция при расследовании преступлений. Караганда, 1978.;

174 Лузгин ИМ. Моделирование при расследовании преступлений. М., 1981.

175 Глазырин В.Ф. Психологические особенности следственного эксперимента. Следственные действия. М, 1994. С. 208-212

176 Бобраков И.А. Воздействие преступников на свидетелей и потерпевших и криминалистические методы его преодоления: Автореф. дисс.... канд. юрид. наук. М., 1997. С. 15.

177 Марченко С.Л. Обеспечение безопасности участников уголовного процесса: Автореф. дисс.... канд. юрид.наук. М.,1994. С. 15-16.

178 Андреев В. И. Проблемы обеспечения безопасности лиц, участвующих в уголовном процессе Республики Казахстан: Дис. … канд. юрид. наук. — Караганда, 2001. — 160 с.

179 Гинзбург А.Я, Опознание в следственной, оперативно-розыскной и экспертной практике: Учебно-практическое пособие /Подред. Р.С. Белкина. М., 1996. С. 17-18.

180 Григорьев В.Н, Расследование преступлений в чрезвычайных условиях. М., 1994. С. 161-164

181 Кочаров Г.И. Опознание на предварительном следствии. М., 1955.;

182 Леей А.А., Пичкалева Г.И., Селиванов Н.А. Проверка и получение показаний следователем. М., 1987. С. 35-63.

183 Закон Республики Казахстан «О судебной экспертизе» от 12 ноября 1997 г. № 188 (с изменениями от 5 мая 2000 г. и от 6 ноября 2001 г.) // Казахстанская правда. 2001. 17 нояб.

184 Аубакиров А. Ф., Гинзбург А. Я., Лифшиц Ю. Д. Значение экспертизы в расследовании преступлений / Под общ. ред. Л. В. Винницкого. — Караганда: Карагандинская высшая школа МВД СССР, 1991. — 100 с.

185 Аубакиров А. Ф., Гинзбург А. Я. Криминалистика: криминалистическая тактика: Учебник. — Алматы: ТОО Центр деловой книги «Глобус», 2003. — 432 с.