МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
ИМЕНИ БАРИМБЕКА БЕЙСЕНОВА

УДК 343.13:004 (574)

На правах рукописи

СЫРБУ АЛЕКСАНДР ВЛАДИМИРОВИЧ

ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ С ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

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

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель:
кандидат юридических наук,
доцент
К. В. Ким

Караганда, 2005

СОДЕРЖАНИЕ

стр.

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие стандарты:

1. ГОСТ 16487-70. Делопроизводство и архивное дело. Термины и определения. Введ. 01.01.71 г. — М., 1971. — 43 с.
2. ГОСТ 6.10.12-75. Унифицированные системы документации. Термины и определения. Введ. 1975-01-01. — М., 1975. — 36 с.
3. ГОСТ 6.10.4-84. Придание юридической силы документам на машинном носителе и машинограммах, создаваемым средствами вычислительной техники. Введ. от 09.10.84 г. — М., 1984. — 51 с.
4. ГОСТ 15971-84. Информационное обеспечение АСУ. Термины и определение. Введ.01.01.85 г. — М., 1985. — 32 с.
5. РД 50-613-86. Методические указания по внедрению и применению ГОСТа 6.10.4-84 УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения. — М., 1986. — 15 с.
6. Государственный стандарт РФ 7.0-99. Информационно-библиотечная деятельность, библиография. Термины и определения. — М., 1999. — 41 с.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

УПК — Уголовно-процессуальный кодекс
РК — Республика Казахстан
УВД — Управление внутренних дел
ЭВМ — электронно-вычислительная машина
ОРД — оперативно-розыскная деятельность
п. — пункт
ч. — часть
ст. — статья
УК — Уголовный кодекс
МВД — Министерство внутренних дел
ГОСТ — государственный стандарт
ОРИ — оперативно-розыскная информация
ОРМ — оперативно-розыскные мероприятия
СССР — Союз Советских Социалистических Республик
файл — именованная область носителя компьютерной информации
РФ — Российская Федерация
УССР — Украинская Советская Социалистическая Республика
КазССР — Казахская Советская Социалистическая Республика
США — Соединенные Штаты Америки
ФБР — Федеративное бюро расследований
ПК — персональный компьютер
ПЭВМ — персональная электронно-вычислительная машина
Мб — мегабайт
Кб — килобайт
ФРГ — Федеративная Республика Германия
Прокурор — должностное лицо, осуществляющее в пределах своей компетенции надзор за законностью оперативно-розыскной деятельности, дознания, следствия и судебных решений, а также уголовное преследование на всех стадиях уголовного процесса. Полномочия прокурора при досудебном производстве и рассмотрении дела судом определяются соответственно ст. ст. 190, 192 (ч. ч. 6 и 7), 197, 289, 317, 396 (ч. 3), 458, 460 УПК РК.
Канал связи — часть сети, связывающая между собой каждую пару ее оконечных терминалов и состоящая из технических средств передачи и приема данных, включая линию связи, а также средств программного обеспечения и протоколов. В зависимости от характера, принципа построения, назначения и использования, различают каналы проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной, аналоговой, цифровой, дуплексной (двухсторонней) связи и так далее.
LOG-файл — файл регистрации входящей, исходящей информации

ЭВТ — электронно-вычислительная техника
ОЗУ — оперативное запоминающее устройство
ВЗУ — внешнее запоминающее устройство
ООН — Организация Объединенных Наций
СОРМ — специальные оперативно-розыскные мероприятия
АРМ — автоматизированное рабочее место
НИИ — научно-исследовательский институт
ОМП — осмотр места происшествия
СМУ — судебно-экспертные учреждения
СУБД — система управления базами данных

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. В своем Послании к народу Республики Казахстан Президент Н. А. Назарбаев указал, что одной из первоочередных задач, стоящих перед нашим государством, выдвигается «... создание реального правового государства, где все живут по законам ...» [1]. В Концепции правовой политики государства одним из направлений определена реализация принципов обеспечения защиты прав и свобод человека. Так как правовое государство — это государство с высоким уровнем правосознания и правовой культуры в обществе, где правовые нормы не должны противоречить нравственным, то есть основной задачей отправления правосудия должна быть защита прав и законных интересов человека и гражданина.

В условиях, когда преступность приобретает все более организованные формы, а преступления совершаются законспирированными и технически оснащенными группами, актуальной является задача совершенствования уголовно-процессуальных средств, обеспечивающих установление объективной истины и защиту конституционных прав и интересов граждан. В настоящее время эффективно бороться с преступностью невозможно без максимального использования достижений технической науки, как в следственной, так и в оперативно-розыскной деятельности. Это сложная комплексная проблема, включающая многие самостоятельные аспекты исследования. Оптимизация процесса получения и использования информации с технических каналов связи при доказывании — один из них.

Как отметил Президент Республики Казахстан в своем Послании народу Казахстана: «процесс глобализации и научно-технического прогресса, особенно в развитии новых информационных и телекоммуникационных технологий, представляет уникальные возможности для нашей большой, но малонаселенной страны. Телефоны, факсы и электронная почта являются жизненно важными и объективно необходимыми условиями для развития современного бизнеса. Являясь более “интернациональными” и гибкими по своей сути, информационные технологии, в сравнении с другими видами, в большей мере способствуют развитию бизнеса, поддерживают функционирование рыночных механизмов через расширение доступа и осуществление передачи информации» [2, 70-97]. Внедрение высокотехнологических наукоемких производств и развитие рыночных отношений в нашей республике закономерно повлекло широкое использование компьютерных технологий и, как следствие этого, одним из стратегических направлений развития Казахстана определена необходимость «укрепления национальной безопасности за счет проведения гибкой внешней политики, соблюдения национальных интересов путем обеспечения защиты и контроля над государственными информационными ресурсами» [3, 32].

Введение в действие 1 января 1998 г. Уголовно-процессуального кодекса Республики Казахстан заставило по-новому пересмотреть устоявшиеся взгляды на некоторые институты процессуального права, поставило перед необходимо-

стью разработки новых правовых институтов, позволяющих расширить доказательственную базу путем использования в доказывании информации, полученной с технических каналов связи, в том числе с компьютерных систем. Впервые в уголовно-процессуальном праве предусмотрена возможность проведения нового следственного действия — «перехват сообщений», закрепленного в ст. 236 УПК РК. Положения статьи регламентируют основания и порядок принятия решения о производстве перехвата сообщений, определяют органы, исполняющие данное решение, и способ передачи полученной информации следователю. Кроме того, законодатель включает в положения данной статьи производство дополнительного действия — снятие информации с компьютерных систем.

Вопросы, связанные с получением и использованием информации с технических каналов связи в уголовном судопроизводстве, являются актуальными в теоретическом и практическом аспектах, что обусловлено рядом факторов.

1. В теории отечественного уголовно-процессуального права отсутствуют исследования, раскрывающие понятие и содержание сущности назначения и порядка получения и использования информации с технических каналов связи.

2. Существующая нормативная правовая база, регулирующая получение и использование информации с технических каналов связи, требует дальнейшего совершенствования. Так, в нормах уголовно-процессуального права не раскрыты такие понятия как: перехват сообщений, технические каналы связи, компьютерные каналы связи, компьютерные системы, снятие информации, носитель информации, понятие и виды информации, документ, виды документов и другое. Закрепление вышеуказанных понятий и терминов в Уголовно-процессуальном кодексе позволило бы определить пределы вторжения сотрудников правоохранительных органов в компьютерные базы данных физических и юридических лиц, доказательственное значение их деятельности; способы и порядок получения необходимой информации, средства и способы ее фиксации и сортировки; содержание процессуального порядка доступа отдельных лиц к различным видам информации, а также их процессуальные полномочия.

Указанные обстоятельства ставят вопрос и о необходимости установления особых сроков и условий получения и использования информации с технических каналов связи. Большие затруднения на практике вызывают вопросы содержания понятий «перехват сообщений» и «снятие информации». Является ли это копированием, полным или частичным изъятием, отделением части информации и недопущение ее к адресату в совокупности, либо каждое из этих действий является самостоятельным и имеет свои цели? Включает ли перехват сообщений действия по производству компьютерного розыска, обыска в компьютерных системах, выемки информации, осуществлению ее осмотра, взламыванию паролей? Возникают вопросы и о продолжительности данных действий: «Необходимо ли получать санкцию прокурора каждый раз перед проведением перехвата сообщений, либо единожды по уголовному делу?».

Проблемы, связанные с получением и использованием информации с технических каналов связи, в уголовном судопроизводстве имеют место и в требованиях, предъявляемых к материальному закреплению информации. В частно-

сти, определение процессуального содержания терминов: «носитель информации», «документ», позволит в полной мере устанавливать признаки и свойства информации в них заключенных, способы ее оформления и введения в процесс доказывания.

Из указанного следует закономерный вывод о том, что успешное регулирование порядка получения и использования информации с технических каналов связи в процессе расследования напрямую зависит от совершенствования уголовно-процессуального законодательства в этой сфере и разработки обоснованной научной базы.

Кроме того, в уголовно-процессуальных нормах в полной мере не отражен механизм производства исследуемого следственного действия. Отсутствует логическая согласованность между действиями, составляющими данный механизм. Получение и использование информации с технических каналов связи в уголовно-процессуальном праве является проблемой, требующей своего подробного исследования. Недостаточная уголовно-процессуальная регламентация перехвата сообщений, является одной из причин того, что из 300 исследуемых уголовных дел (см. Приложение А) о фактах незаконного проникновения в компьютерную систему или сеть; неправомерного доступа к компьютерной информации; хищений вычислительной техники; использования вредоносных программ для ЭВМ; хищений, совершенных с использованием ЭВМ, перехват сообщений не проводился.

Данное обстоятельство может свидетельствовать о больших затруднениях правоприменителя, связанных с реализацией норм по перехвату сообщений. Кроме того, респондирование (см. Приложение Б) по данному вопросу 120 следователей, 80 дознавателей, 50 прокурорских работников, 57 специалистов, 23 экспертов свидетельствует о том, что о сущности и механизме перехвата сообщений имеют представление лишь 28 % опрошенных.

Думается, указанные проблемы применения уголовно-процессуального законодательства, будучи объективным результатом незначительного срока правовой адаптации уголовно-процессуальной новеллы, являются самостоятельным основанием необходимости научного исследования получения и использования информации с технических каналов связи в уголовном судопроизводстве.

3. Уголовно-процессуальное право Республики Казахстан нуждается в подробном анализе всех норм, связанных с использованием научно-технических достижений, рецепцируемых из практики зарубежного законодательства на предмет их соответствия основам отечественного права и возможности использования в нашем уголовном судопроизводстве. Эмпирические исследования показали, что нормы, регулирующие применение компьютерных технологий при получении и использовании информации с технических каналов связи, почти не применяются в практике расследования уголовных дел. Полагаем, что настоящий факт может быть обусловлен объективными и субъективными закономерностями уголовно-процессуальной деятельности на современном этапе нашей республики. В связи с чем, необходимо выявить и исследовать данные закономерности и разработать рекомендации, направленные на совершенство-

вание законодательства и механизма его реализации по вопросам получения и использования информации с технических каналов связи.

Следует отметить, что каждая из указанных причин уже является основанием для проведения исследования проблемы получения и использования информации, получаемой с технических каналов связи в процессе расследования.

Теоретическая и практическая значимость исследования обусловлена проводимой судебно-правовой реформой и социальной востребованностью научно обоснованного анализа норм уголовно-процессуального законодательства. Вышеизложенные факторы, безусловно, подтверждают обоснованность выбора темы и ее актуальность.

Цели и задачи исследования. Целью настоящего исследования является раскрытие процессуального значения сущности и содержания информации, передаваемой по техническим, в том числе компьютерным каналам связи, порядка ее использования; раскрытие назначения и роли перехвата сообщений как самостоятельного следственного действия в системе следственных действий уголовно-процессуального права Республики Казахстан; а также разработка на данной основе рекомендаций, направленных на совершенствование уголовно-процессуальной регламентации получения и использования информации с технических каналов связи.

Для реализации данной цели были определены следующие задачи:

- исследовать компьютерные системы и технические каналы связи как объекты уголовно-процессуальных действий и источники получения доказательственной информации в процессе расследования преступлений;
- определить основные процессуальные способы получения информации с технических каналов связи и их значение в процессе расследования;
- провести уголовно-процессуальный анализ перехвата сообщений как нового следственного действия с точки зрения его познавательной структуры;
- исследовать порядок производства перехвата сообщений и разработать рекомендации по его совершенствованию, выделить виды перехвата сообщений;
- раскрыть содержание терминов, используемых при получении и использовании информации с технических каналов связи в уголовном судопроизводстве;
- провести анализ практики реализации норм по получению и использованию информации с технических каналов связи и снятии информации с компьютерных систем и разработать рекомендации по их законодательному совершенствованию;
- исследовать правовые, организационные и тактические особенности привлечения специальных познаний в различных формах обнаружения, изъятия, фиксации и использования информации в технически каналах связи;

– на основе исследования теоретического, нормативного, эмпирического материала, его анализа разработать рекомендации, направленные на совершенствование практики реализации получения и использования информации с технических каналов связи, оптимизацию практики перехвата сообщений;
– рассмотреть особенности назначения судебно-компьютерной экспертизы.

Объект и предмет исследования. ***Объектом*** данного исследования является деятельность по применению норм по получению и использованию информации с технических каналов связи в уголовном судопроизводстве.

Предметом исследования выступают нормы Конституции РК, уголовно-процессуального законодательства, других нормативно-правовых актов Республики Казахстан, регламентирующие вопросы получения и использования информации с технических каналов связи в уголовном судопроизводстве, а также отношения, возникающие в процессе их реализации. Кроме того, предметом изучения явились аналогичные нормы зарубежного права, имеющего значение для уголовно-процессуального законодательства, материалы практики следствия, дознания, прокуратуры, суда, экспертной деятельности по рассматриваемым вопросам.

Теоретическую базу исследования составили труды таких ученых, как: М. А. Арыстанбеков, А. Н. Ахпанов, К. Ж. Балтабаев, Ю. М. Батурин, Д. И. Бедняков, Р. С. Белкин, А. Я. Гинзбург, Ю. Гульбин, А. М. Жодзишский, К. В. Ким, М. Ч. Когамов, А. П. Кузьмин, Р. А. Назмышев, Б. М. Нургалиев, С. С. Овчинский, И. Л. Петрухин, Г. И. Поврезнюк, В. Ю. Рогозин, Б. Х. Толеубекова, И. Я. Фойницкий, А. А. Чувилев, А. Д. Шаймуханов, А. Ю. Шумилов, П. С. Элькинд, Р. Х. Якупов и других.

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, моделирования, системно-структурного, деятельностного подхода, исторического, сравнительно-правового, социологического, анкетирования и других.

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

Эмпирическую базу составили результаты опросов 50 работников прокуратуры и 200 работников следствия, дознания, 80 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 1998-2004 гг. Сбор эмпирическо-

го материала проводился на территориях Центрального, Восточного, Западного, Южного и Северного регионов Республики Казахстан.

Научная новизна диссертационного исследования. Стремительное развитие информационных технологий приводит к тому, что многие явления социальной жизни все в большей мере находят отражение в так называемых «виртуальных мирах», то есть в тех информационных средах, носителями которых выступают как средства массовой информации, так и глобальные компьютерные телекоммуникационные сети и системы. Одновременно вместе с расширением диапазона применения уже существующих ЭВМ совершенствуются сами технические возможности машин, многократно расширяющие этот диапазон.

В силу того, что организованная преступность в настоящее время оказывает возрастающее влияние на самые разные стороны социальной, экономической и политической жизни общества, борьба с ней должна предусматривать применение всех возможных научных средств и методов. Эта борьба естественным образом должна охватывать «информационные сферы», которые включают в себя, в первую очередь, средства массовой информации, а также средства телекоммуникаций и связи, глобальные компьютерные сети, базы данных и индустрию самых разнообразных информационных услуг, которые являются важным источником информации в процессе расследования преступлений.

В уголовно-процессуальной науке Республики Казахстан отсутствуют исследования, посвященные самостоятельному изучению проблемы перехвата сообщений, вопросам о тактических и организационных аспектах процессуальных способов собирания доказательственной информации с технических каналов связи, а также снятию информации с компьютерных систем. В этой связи, научная новизна исследования заключается в том, что на монографическом уровне впервые осуществлено комплексное изучение перехвата сообщений как самостоятельного уголовно-процессуального действия.

Актуальной остается задача разработки и представления в распоряжение практикующих юристов теоретических основ процессуального порядка собирания информации с технических каналов связи и научно-обоснованных рекомендаций по организации и тактике получения и использования информации при перехвате сообщений (см. Приложение В). Очевидно, что в такой проблемной ситуации требуется восполнить дефицит научных познаний, связанных с получением и использованием информации с технических каналов связи в уголовном судопроизводстве. Отметим, что настоящее совершенствование может быть основано только на фундаментальных научных исследованиях получения и использования информации с технических каналов связи в уголовном судопроизводстве, каким может быть диссертационное исследование настоящей темы.

Диссертантом сформулированы новые теоретические положения, направленные на определение сущности и значения получения информации с технических каналов связи, в том числе перехвата сообщений, совершенствование

законодательного регламентирования, а также практики его применения в стадиях досудебного производства, оптимизацию расследования уголовных дел.

Основные положения, выносимые на защиту:

1. Компьютерные системы и объединяющие их технические каналы связи, как объекты процессуальных действий, являются носителями огромного объема информации, могущей иметь значение для расследуемых дел. Исследование и анализ специальной литературы позволили определить специфические источники получения доказательственной информации: компьютерная система, канал связи, линия связи.

Полученная при перехвате сообщений с компьютерных систем и технических каналов связи компьютерная информация может иметь типичные и факультативные свойства, которые используются для идентификации файла и находящейся в нем информации. Обозначенные свойства файлов при отражении их в протоколах следственных действий позволяют удостоверить относимость, допустимость и достоверность полученной информации при ее дальнейшем использовании в качестве доказательства при расследовании уголовных дел.

2. Основными процессуальными способами обнаружения, изъятия информации, передаваемой по техническим, в том числе компьютерным каналам связи являются: осмотр, выемка, розыск в компьютерных сетях, перехват сообщений, назначение и производство судебных экспертиз. Основным объектом исследования данных действий выступает электронный документ, который должен:

- создаваться, обрабатываться, храниться, передаваться и приниматься с помощью программных и технических средств;
- содержать реквизиты, позволяющие подтвердить его подлинность и целостность;
- быть отображенным (воспроизведенным) в форме, понятной для восприятия человеком.

3. Под перехватом сообщений, передаваемых по техническим и компьютерным каналам связи, следует понимать действия органа уголовного преследования, а также физических или юридических лиц по поручению органа уголовного преследования, направленные на копирование, блокирование, изъятие и уничтожение передаваемой информации, с целью получения доказательств по делу.

Перехват сообщений является самостоятельным следственным действием, поскольку имеет отличные от других следственных действий цель, объект, метод, условия, задачи, порядок и условия проведения, где:

- целью перехвата сообщений является обнаружение информации в технических каналам связи, об обстоятельствах, подлежащих доказыванию по уголовному делу;
- к задачам перехвата сообщений относятся: копирование, блокирование, изъятие, уничтожение информации;
- объектом перехвата сообщений являются — компьютерная система, компьютерная сеть, технические каналы связи;

– к условиям производства перехвата сообщений относятся: процессуальные, организационные и тактические особенности, продолжительность срока перехвата сообщений; юридические и фактические основания его производства; порядок санкционирования; способы обнаружения, фиксации и исследования полученной информации.

4. Перехват сообщений, передаваемых по техническим, в том числе компьютерным каналам связи, и снятие информации с компьютерных систем должен реализовываться в следующем порядке:

– определение цели и оснований для производства перехвата сообщений;
– определение объекта и системы, в которой планируется производство перехвата;
– определение участников проводимого действия;
– определение срока и порядка передачи перехваченной информации;
– определение вида перехвата сообщений;
– вынесение постановления;
– санкционирование постановления прокурором;
– получение перехваченной информации от исполняющего органа;
– осмотр полученной информации и принятие решения о ее дальнейшей судьбе.

Перехват сообщений можно разделить по времени проведения на разовый и продолжительный, в которых выделены их процессуальные и организационно-тактические особенности.

5. Правильное осуществление получения и использования информации с технических каналов связи и компьютерных систем зависит от однозначного понимания следующих терминов: компьютерная информация, подлинник, копия, машинограмма, электронный документ, машиночитаемый документ, материальный носитель, машиночитаемый носитель, человекочитаемый (твердый) носитель, личная информация, информация персонального характера, документ, процессуальные документы, иные документы, официальные документы, частные документы, компьютер, персональный компьютер, ЭВМ, компьютерная система, вычислительная система, локальная система, автоматизированная система, система ЭВМ, компьютерная сеть, сеть ЭВМ, локальная сеть, глобальная сеть, канал связи, линия связи, электрическая связь, сети электросвязи. В работе раскрыто содержание и даны определения перечисленных терминов.

6. Анализ практики реализации норм о получении информации с технических каналов связи и компьютерных систем, а также теоретическое и нормативное исследование, позволили диссертанту разработать рекомендации по совершенствованию законодательной регламентации применения данного действия.

В частности, предлагается дополнить ст. 236 УПК РК десятью новыми частями (3-11, 13) и изложить ее в следующей редакции:

«1. Перехват сообщений, передаваемых по техническим, в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации, относящейся к расследуемому делу, производятся на основании постановления сле-

дователя, санкционированного прокурором с целью получения информации об обстоятельствах, имеющих значение для дела.

2. Постановление следователя о производстве перехвата сообщений должно содержать номер уголовного дела и основания, по которым должно производиться данное действие, данные о лице, чьи сообщения подлежат перехвату. В постановлении должны быть указаны сроки передачи относимой к делу информации, вид канала связи, либо компьютерной системы, которая должна контролироваться.

3. Перехват сообщений и снятие с компьютерных систем информации производится на основании фактических данных, дающих основание полагать, что в информации, поступающей и отправляемой подозреваемым, обвиняемым, могут содержаться сведения, имеющие значение для дела, а также для своевременного предотвращения готовящихся преступных деяний.

4. Перехват сообщений потерпевшего, свидетеля и других участников уголовного процесса допускается при наличии угрозы совершения насилия, вымогательства либо других противоправных действий в отношении этих лиц на основании соответствующего заявления или с их согласия на перехват сообщений.

5. Перехват сообщений свидетелей, потерпевших, других участников уголовного процесса, допускается без их согласия при наличии информации о том, что они совершают действия по укрывательству преступления, орудий и средств совершения преступления, предметов, добытых преступным путем, препятствуют установлению истины по делу, обмениваются информацией с подозреваемым, обвиняемым.

6. Перехват сообщений, передаваемых по техническим, в том числе и компьютерным, каналам связи, и снятие с компьютерных систем информации устанавливается на срок до двух месяцев. Дальнейшее продление срока производится в соответствии с положениями ч. ч. 4, 5, 6, 7 ст. 196 УПК РК.

7. О приостановление перехвата сообщений указывается в постановлении о приостановлении предварительного следствия или в отдельном Постановлении “О приостановлении производства перехвата сообщений”, вынесенном следователем, дознавателем, прокурором.

8. Производство перехвата сообщений прекращается по постановлению следователя, дознавателя, прокурора, если необходимость в данной мере отпадает, но не позднее окончания расследования по данному уголовному делу.

9. Возобновление производства перехвата сообщений производится на основании положений ч. ч. 1, 2 ст. 268 УПК РК или наряду с возобновлением предварительного следствия. В постановлении должно быть указано — сохраняется ли прежний режим перехвата сообщений или изменяется. Установленные изменения указываются в выносимом постановлении.

10. Постановление следователя, санкционированное прокурором, направляется для исполнения органу, осуществляющему ОРД или администрации телефонного узла, телефонной станции, организациям и учреждениям, осуществляющих предоставление услуг по работе в компьютерных сетях.

11. Санкция на перехват сообщений абонентов в пределах населенного пункта дается районным, городским прокурором или их заместителями; в пределах области или территории Республики Казахстан — прокурорами областей и приравненных к ним прокурорами.

12. Сообщения и компьютерная информация, полученные в результате перехвата, фиксируются специалистом на соответствующем носителе и передаются следователю в опечатанном виде с указанием даты, времени перехвата и краткой характеристики использованных при этом технических средств.

13. Полученная при перехвате сообщений информация копируется на машинный носитель, после чего, по решению органа уголовного преследования может быть направлена адресату, блокирована, изъята или уничтожена. Операции, проводимые над информацией, отражаются в протоколе осмотра предметов и документов, согласно требованиям, установленными ст. ст. 221, 222, 223, 227 УПК РК».

7. Исследование и анализ нормативной, специальной литературы, а также практики привлечения специалистов в расследование позволило сделать предложение по совершенствованию законодательства.

Дополнить УПК РК ст. 217-1 «Допрос специалиста», изложив ее в следующей редакции: «Если необходимо уточнить примененные специалистом методы и термины, а также выяснить ряд других вопросов, связанных с участием специалиста при проведенном следственном действии, следователь (дознаватель) вправе допросить специалиста.

Перед началом допроса специалисту разъясняются его права и обязанности, и он предупреждается об ответственности за заведомо ложные показания по ст. 352 УК РК.

Протокол допроса специалиста составляется с соблюдением правил, предусмотренных ст. 218 УПК РК.

В случае необходимости получения сведений консультативного, справочного характера следователь (дознаватель) может пригласить специалиста для их получения. Предоставление сведений, носящих специальный характер, оформляется в виде справки, подписанной специалистом. К справке могут быть приложены схемы, таблицы, графики и другие материалы. Приложение подписывается специалистом».

Определяя, что исследование специалиста может выступать как самостоятельный источник доказательств, основание для производства экспертизы, способ получения доказательственной информации, предлагается дополнить УПК РК ст. 251-1 «Исследование специалиста», изложив ее в следующей редакции: «Исследование, проводимое специалистом, производится в случаях, когда обстоятельства, имеющие значение для дела, могут быть получены на основе специальных знаний до производства экспертизы. Полученные результаты, не освобождают лицо, ведущее уголовный процесс, от необходимости в соответствующих случаях назначить экспертизу.

Ход и результаты исследования отражаются в протоколе исследования, приобщаемом в качестве приложения к протоколу следственного действия (ч. 8 ст. 203 УПК РК).

Протокол исследования — письменный документ, в котором отражены выводы по вопросам, поставленным перед специалистом, основанные на результатах проведенного с использованием специальных знаний исследования. В протоколе должно быть указаны: когда, где, кем проведено исследование, какие материалы уголовного дела им исследованы; в рамках какого следственного или судебного действия он участвовал; какие объекты были подвергнуты исследованию; какие исследования произведены; какие методы и средства применены и в каком виде они надежны; если при исследовании специалист установит обстоятельства, имеющие значение для дела, по поводу которых ему не было изложено в задании, он вправе указать их в своем документе.

К протоколу исследования прилагаются исследованные объекты, а также фототаблицы, графики, модели, слепки, оттиски, схемы и другие материалы, подтверждающие выводы специалиста. Данный документ подписывается специалистом и лицами, присутствующими при исследовании».

Исключить п. 5 ч. 1 ст. 96 УПК РК: «Если он участвовал в деле в качестве специалиста, за исключением случаев участия в соответствии со ст. 224 настоящего кодекса врача-специалиста в области судебной медицины в осмотре трупа человека».

Дополнить ч. 1 ст. 96 УПК РК «Отвод эксперта», пунктами:

«6) если он признан в установленном законом порядке ограниченно дееспособными или недееспособными;

7) если он ранее судим;

8) если он уволен по отрицательным мотивам с должности, связанной с осуществлением судебно-экспертной деятельности».

Дополнить ч. 1 ст. 352 УК РК «Заведомо ложные показания, заключение эксперта или неправильный перевод» после слов «1. Заведомо ложные показания, свидетеля, потерпевшего» словом «специалиста» и далее по тексту.

8. Изучение и анализ судебно-следственной практики Республики Казахстан, а также практики зарубежных стран, исследование их нормативной и теоретической базы позволили диссертанту обосновать необходимость разработки и введения в законодательство Республики Казахстан нормы, регламентирующей розыск в компьютерных сетях (или в среде для хранения компьютерных данных), проводимый с целью обнаружения и изъятия искомой компьютерной информации, которая после надлежащего документирования может стать доказательством при расследовании преступлений.

9. Изучение и анализ специальной литературы, а также судебно-экспертной практики позволили выделить виды судебно-технологической (компьютерной) экспертизы и определить решаемые ими диагностические и идентификационные задачи, содержание которых раскрывается в работе.

Теоретическая и практическая значимость результатов исследования определяется тем, что в работе в комплексе рассматриваются процессу-

альные способы получения и использования информации с технических каналов связи, в том числе и перехвата сообщений как самостоятельного следственного действия. Раскрываются теоретические и правовые основы перехвата сообщений в уголовном судопроизводстве, его содержание, особенности и механизм реализации в процессе расследования преступлений, особенности исследования компьютерной техники и электронной информации, а также исследуется порядок и особенности назначения судебно-компьютерной экспертизы. Кроме того, содержащиеся в диссертации выводы и предложения могут быть использованы:

- в научных исследованиях, направленных на развитие и углубление теории уголовно-процессуального права;
- в нормотворческом процессе при регламентации положений о производстве перехвата сообщений;
- при формулировании понятий терминов, используемых при получении и использовании информации с технических каналов связи;
- при определении правовых гарантий соблюдения прав и интересов физических и юридических лиц при осуществлении органом уголовного преследования снятия информации с технических каналов связи;
- в правоприменительной деятельности органов уголовного судопроизводства при разрешении вопросов, связанных с получением и использованием информации с технических каналов связи и снятии информации с компьютерных систем;
- в учебном процессе высших и специальных заведений юридического профиля.

Апробация и внедрение результатов исследования. Диссертантом подготовлено четырнадцать научных статей, в которых излагаются результаты проведенного исследования, три из которых опубликованы в изданиях, рекомендованных Комитетом по надзору и аттестации науки и образования МОиН РК. Основные положения диссертации докладывались на четырех международных и двух межвузовских научно-практических конференциях: международной научно-практической конференции «Перспективы государственно-правового и социального развития Республики Казахстан», проводимой в Костанайском юридическом институте МВД РК; международной научно-практической конференции «Актуальные проблемы современности», проводимой в Карагандинском институте актуального образования «Болашак»; международной научно-практической конференции «Проблемы уголовно-процессуального права», проводимой в Карагандинском юридическом институте МВД РК имени Баримбека Бейсенова; межвузовской научно-практической конференции «Актуальные проблемы борьбы с преступностью и иными правонарушениями», проводимой в Барнаульском юридическом институте МВД РФ; межвузовской научно-практической конференции, посвященной 10-летию со дня принятия первого закона Республики Казахстан «Об органах внутренних дел»; международной научно-практиче-

ской конференции, состоявшейся на базе кафедры уголовного процесса в Карагандинском юридическом институте МВД РК имени Баримбека Бейсенова».

Теоретические положения и практические рекомендации работы внедрены в учебный процесс по курсу «Уголовно-процессуальное право РК» и дисциплин «Предварительное следствие РК» и «Дознание и предварительное следствие в РК» в Карагандинском юридическом институте МВД РК имени Баримбека Бейсенова, в учебный процесс по курсу «Криминалистика», «Уголовно-процессуальное право» в КазГЮУ г. Астаны, а также используются в практической деятельности органов предварительного следствия и дознания ГУВД, прокуратуры, военного и областного суда.

Структура и объем диссертационного исследования. Структура работы определяется поставленными в диссертации целями, задачами и логикой исследования. Работа состоит из введения, трех разделов, включающих в себя одиннадцать подразделов, заключения, списка использованных источников и приложений. Диссертация соответствует требованиям, предъявляемым Инструкцией Комитета по надзору и аттестации науки и образования МОиН Республики Казахстан и ее объем составляет 172 страницы текста компьютерного набора (приложения в указанный объем диссертации не включаются).

1 ПОНЯТИЕ И ЗНАЧЕНИЕ ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ С ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

1.1 Понятие и виды информации, используемой в процессе расследования преступлений

Термин «информация» широко применяется в уголовно-процессуальной, специальной литературе и трактуется как сообщения, осведомляющие о положении дел, о состоянии чего-нибудь [4, 232; 5, 12]. Данный термин возник в социальной среде и первоначально применялся для обозначения сведений, передаваемых одними людьми другим устным, письменным или иным способом.

Развитие и усложнение информационных процессов вызвало активизацию научного интереса к категории «информация» и привело к необходимости изучения ее содержания. Большинство ученых [6, 300; 7, 50; 8, 40; 9, 200], исследуя сущность информации, исходили, во-первых, из законов материалистической диалектики, а во-вторых — из исследованной В. И. Лениным философской категории отражения. Но в тоже время в философской литературе высказывалось мнение, что категория «информация» применима только при рассмотрении процессов управления. В связи с этим Т. Д. Павлов писал, что информация возникает на определенном уровне организации материи при наличии процессов управления, и что информация существует только в высокоорганизованных системах, какими являются человек, животные, кибернетические устройства, моделирующие в определенной мере деятельность человека [10, 68].

Вместе с тем, предпринимаются попытки рассматривать информацию с аксиологических (ценностных), математических, алгоритмических и других позиций как количественную меру устранения неопределенности (энтропии), меру организаций системы [11, 201; 12, 311]. Так, А. Г. Мамиконов пишет, что «понятие “информация” может быть истолковано как некоторая совокупность сведений, определяющих меру наших знаний о тех или иных событиях, фактах и их взаимосвязи» [13, 83].

Представления об информации как об идеальном социальном феномене [14, 121], стремление ограничить ее только сферой общения между людьми, абстрагирование от всего, что внесли в трактовку понятия информации кибернетика и естественные науки, не учитывают современного состояния проблемы. Возникла множественность аспектов в понимании информации как объективного явления:

- теоретико-отражательный, раскрывающий роль информации в процессах отображения объективной действительности;
- гносеологический, раскрывающий представление об информации как средстве познания;
- семантический, предполагающий содержание и значение информации;

- аксиологический, формирующий концепции ценности информации для различных сфер деятельности;
- количественный, приобретающий значение для принятия решений при определении, например, емкости «памяти» информационно-поисковых систем;
- коммуникативный, раскрывающий сложную организационно-техническую природу информационной связи, и другие [15, 17-19].

Все это обусловило большое количество попыток определения информации как научного понятия.

Каждое такое определение, если оно применяется в сфере своего действия, верно отображает какую-то сторону или особенность информации. Однако всякие попытки универсализации частного определения, открывающего один или несколько аспектов информации, приводят к неудачным выводам. Например, одно из первых определений информации появилось при решении задач теории связи. Естественно, что оно специально было подобрано так, чтобы отвечать запросам этой теории. Как отмечают некоторые исследователи, с точки зрения теории связи количество информации в случае несущественного или даже ложного сообщения и в случае сообщения о величайшем открытии (поскольку они имеют равную длину и требуют равного количества времени на передачу техническими средствами) является одинаковым [16, 23].

Вопросам исследования информации было посвящено множество работ, в связи, с чем существует масса различных определений понятия информация. Например: в ГОСТе 15971-84 определено, что: «Информация — содержание какого либо сообщения, сведения о чем либо, рассматриваемые в аспекте их передачи в пространстве и времени …», «Информация — это значение, вкладываемое человеком в данные на основании известных соглашений, используемых для их представления; сведения, подлежащие передаче» [5, 23]. Полагаем необходимым упомянуть классическое определение К. Шеннона, в соответствии, с которым информация — это то, что сокращает степень неопределенности у ее адресата, о каком-либо объекте. Другими словами, информация — это то, что увеличивает степень знания ее адресатом интересующих его объектов окружающего мира. В указанном контексте количество информации можно даже рассчитать, например, по критерию повышения вероятности успешного решения поставленной задачи.

Возникает естественный вопрос — с чем связано различное представление понятия «информация» разными его пользователями, включая профессионалов? Во-первых, его сложной и неоднозначной сущностью, которая к тому же имеет тенденцию достаточно быстро изменяться в ходе научно-технического прогресса.

Во-вторых, с тем, что цитируемые и другие определения этого понятия вычленяют только те его признаки, которые служат достижению конкретных целей или соответствуют контексту документов, в которых они должны быть опубликованы.

А. Я. Сухарев кратко эти признаки информации сформулировал так: «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» [5, 14].

В то же время следует отметить, что часто «данные» (сведения, факты, показатели, выраженные как в числовой, так и любой другой форме) [5, 11] рассматриваются как синоним термина «информация». Например, в одном из изданий «Словаря терминов по информатике» данные трактуются как «информация, представляющая собой сведения ….», а в ГОСТе 1597-84 как «информация, представленная на материальных носителях». Но если на бытовом уровне смешение понятий «данные» и «информация» вполне допустимо, то для профессионалов это может привести и приводит к серьезным последствиям. В связи с чем, с целью смыслового разделения понятий «информация» и «данные» Ассоциация стандартов Франции дает следующее определение: «Данные — факт, понятие или инструкции, представленные в условной форме, удобной для пересылки, интерпретации и обработки человеком или автоматизированными системами». Таким образом, чтобы стать информацией, данные должны правильно отображать объекты описания, в противном случае мы будем иметь дело с «дезинформацией» (ложной информацией). «Правильность отражения действительности» в соответствии с теорией познания всегда носит условный характер, так как связана с уровнем знаний общества или отдельных его социальных групп и индивидуумов. Необходимо учитывать, что в зависимости от образовательного, возрастного, социального статусов субъекта информирования, а также целей использования (например, для решения научных, технических, производственных и других задач), состав и точность данных, которыми владеют или которые необходимы различным организациям и лицам об одном и том же объекте, будут существенно различаться. В указанном плане данные, которые для одного субъекта будут представляться вполне точными, для другого — могут оказаться грубой «дезинформацией».

Чтобы стать информацией данные должны представлять для субъекта информирования «определенный интерес» и «новизну», то есть для него они должны быть связаны с необходимостью решения практических или других задач и сокращать «степень неопределенности» об объекте интереса. В указанном плане информация помимо «прибавления знаний» об интересующем объекте, должна доставляться своевременно. «Если в наших знаниях о каком-либо предмете, — пишет А. Д. Урсул, — существует неясность, неопределенность, а, получив новые сведения об этом предмете, мы можем уже более определенно судить о нем, то это значит, что сообщение содержало в себе информацию» [17, 32]. Если сообщение не снижает неопределенности, то с позиций рассматриваемой теории предполагается, что в нем не содержится информации. На основе вышеизложенного и применяя понятие «информации» в сфере уголовного су-

допроизводства можно констатировать, что качественная сторона оперативной и следственной информации раскрывается через ее количество, которое содержит суждения по исследуемой ситуации и обладает степенью истинности (доказанности), в какой-то мере уменьшающей неопределенность. Следовательно, чем больше неопределенности устраняет сообщение, тем больше содержит оно информации.

Данный подход наглядно объясняет информационные процессы, характерные для раскрытия преступлений, когда проверка версий влечет за собой устранение одной неопределенности и возникновение новой до тех пор, пока полученные сведения не снимут общего состояния неопределенности. Изложенное относится и к оперативно-розыскным, и к следственным версиям, различие между которыми признается в теории криминалистики. По мнению А. М. Ларина, в случаях, «когда оперативные данные исходят из независимых друг от друга источников, когда применены различные методы их сбора, когда используются научно-технические средства, оперативные данные могут быть весьма точными. Если эти данные согласуются с содержанием материалов дела и дают правдоподобное объяснение обстоятельствам, зафиксированным процессуальным путем, они, по мнению автора, используются для построения следственной версии, но не в качестве основания, а как объясняющая часть» [18, 60].

Анализируя уголовно-процессуальное законодательство можно сказать, что в УПК РК термин «информация» является аксиоматичным и включает в себя такие термины как «фактические данные», «сведения», «оперативно-розыскная информация». Возникает вопрос: «Что понимать под фактическими данными и оперативно-розыскной информацией?». Мнения, которые были высказаны учеными-процессуалистами по перечисленным вопросам, можно условно объединить в несколько групп.

К первой можно отнести тех ученых, которые считают, что фактические данные — есть факты объективной действительности [19, 15; 20, 24-25].

Другие ученые понимают под фактическими данными доказательства, которыми устанавливаются или опровергаются обстоятельства, подлежащие доказыванию, и источники, из которых субъекты доказывания такие данные получают [21, 83; 22, 78]. Полагаем, что в данном случае речь идет о фактических данных, содержащихся в составленных в соответствии с правилами Уголовно-процессуального кодекса протоколах следственных действий (ч. 1 ст. 122 УПК РК), а также в иных процессуальных документах.

Следующей, наиболее распространенной, является точка зрения о том, что фактические данные — это полученные из законных источников сведения о фактах. Данная точка зрения воспринята большинством ученых-криминалистов [23, 28; 24, 69; 25, 96].

В процессуальной литературе формируется еще один взгляд на фактические данные. Сущность его в том, что сведения о фактах (информации), полученные из предусмотренных в законе источников, это еще не есть доказательство, а «доказательственная информация» [26, 29], «исходные доказательствен-

ные данные» [27, 16]. При этом доказательство понимается в качестве достоверно доказанного знания. Это происходит только в тот момент, когда информация, содержащаяся в предусмотренных законом источниках, используется при принятии основных процессуальных решений.

Таковыми являются основные позиции по вопросам определения фактических данных.

В то же время полагаем необходимым уяснить содержание изначальных терминов «факт», «фактический», «данные», которыми оперирует законодатель, так как «словам и выражениям закона следует придавать то значение, которое они имеют в соответствующем литературном языке» [28, 39].

Термин «факт» употребляется в двух значениях:

1) действительное, не вымышленное явление, событие, происшествие — то, что произошло на самом деле;
2) действительность, реальность — то, что объективно существует.

Термин «фактический» — относящийся к факту (в первом и во втором значении), действительный, соответствующий фактам [29, 1214].

Термин «данные» является синонимом слова «сведения» и означает известие, извещение, сообщение о ком или о чем-либо, характеризующее кого или что-либо, а также осведомленность или знакомство с чем-либо [29, 275]. Также ГОСТом 7.0-99 термин «данные» определяется как «информация, обработанная и представленная в формализованном виде для дальнейшей обработки».

Таким образом, можно считать, что, оперируя термином «фактические данные», законодатель имеет в виду данные о фактах, сведения о фактах, информацию, поскольку прилагательное «фактическое» в данном случае в тексте ст. 16 Основ и ст. ст. 24, 115, 116, 122, 126, 128 УПК РК относится не к самим фактам, а к сведениям об этих фактах. На основе чего следует вывод, что фактические данные и информация в уголовном процессе являются тождественными понятиями.

Одним из видов информации, вовлеченной в уголовный процесс, является оперативно-розыскная информация (далее — ОРИ), рассматривая которую, как результат оперативно-розыскной деятельности (далее — ОРД), В. И. Зажицкий полагал, что это — «различные сведения (данные, информация) об обстоятельствах совершения преступления и лицах, причастных к нему, полученные оперативно-розыскным путем в рамках конкретного дела оперативного учета и зафиксированные в оперативно-служебных материалах: в справках (рапортах) оперативного сотрудника, проводившего оперативно-розыскные мероприятия; в сообщениях конфиденциальных источников; в заключениях различных предприятий, учреждений, организаций, а также от должностных лиц; в материалах фото-, киносъемки, звуко-, видеозаписях, произведенных в процессе оперативно-розыскных мероприятий; в различных материальных предметах, изъятых при осуществлении оперативно-розыскных мероприятий, и т. п.» [30, 110].

В. А. Лукашов содержание оперативно-розыскной информации раскрывает путем перечисления, но уже других компонентов: «сведения, характеризующие оперативно-тактическую обстановку; текущие профилактические и оперативно-

розыскные мероприятия; виды и способы совершения преступлений; приметы преступников, похищенных вещей; психологические черты лиц, подозреваемых в подготовке и совершении преступлений; сведения о замышляемых и подготавливаемых преступлениях, об обстоятельствах, имеющих непосредственное или потенциальное значение для планирования и осуществления оперативно-розыскных мероприятий, проведения оперативно-аналитической работы, а также оказания содействия предварительному расследованию» [31, 7-8].

В ходе расследования органом уголовного преследования может быть получена информация как открытого, так и закрытого характера. Говоря об информации с ограниченным доступом, следует акцентировать внимание на сведениях секретного характера, полученных при производстве дознания и следствия. Данная информация, используется и хранится в соответствии с положениями нормативных правовых актов, регулирующих порядок обращения с данным видом информации. В тех случаях, когда полученные сведения секретного характера не являются вещественными доказательствами по делу, они направляются через спецчасти в отделы, ведающие секретными документами, в организации и учреждения по их принадлежности [32].

Также в сферу уголовного процесса может быть вовлечена и информация персонального характера, под которой понимают сведения о политических взглядах, философских, религиозных и других убеждениях, о принадлежности к политическим партиям, общественным движениям и ассоциациям, личной жизни, включая интимные ее стороны и сексуальное поведение, сведения о национальности, о состоянии физического и психического здоровья, о потреблении алкоголя и иных наркотических и токсических веществ, вкладах в банке, других видах собственности, а также сведения о погашенной судимости; сведения, данные о гражданах и организациях, затрагивающих их интересы и запрещенные для распространения без их согласия [4, 230; 5, 23; 33, 91; 34, 55].

В связи с проблемой «обогащения» оперативно-розыскной информации С. Овчинский предлагает рационально классифицировать информацию и, кладя в основу классификации принцип соотношения целей оперативно-розыскной деятельности, предлагает следующие «типы информации:

1. Информация, имеющая универсальное значение: для прогнозирования индивидуального поведения, профилактики и раскрытия преступлений. Этот вид информации образуется вокруг факторов, влияющих на оперативную обстановку, и характеристик личности тех, кто при определенном стечении обстоятельств может совершать преступления (лица, представляющие оперативный интерес). Он возникает в связи с социальными явлениями, имеющими криминогенный характер, но наряду с ними отражает объективные явления, остающиеся до поры до времени нейтральными для оперативно-розыскной деятельности (например, описание внешности, увлечений, интересов, круга общения изучаемых лиц).

2. Информация, обеспечивающая форму уголовно-процессуальной деятельности — доказывание. Она порождается обстоятельствами преступления и последующими действиями преступников, их соучастников и других прикосно-

венных лиц. Ее содержание — фактические данные, указывающие на событие преступления, действия преступников, обстоятельства, отягчающие или смягчающие их вину, и иные категории, охватываемые предметом доказывания. Если целевое назначение первого вида информации применительно к раскрытию преступлений заключается в том, чтобы заранее определить круг лиц, которые могут оказаться преступниками, то назначение второго вида информации — обеспечить обнаружение лиц, совершивших или совершающих конкретные преступления, получение доказательств их виновности. Ко второму классу следует также отнести информацию, обеспечивающую розыск лиц, уклоняющихся от следствия, суда и совершивших побег из-под стражи» [15, 90].

Рассмотрев вышеозначенные виды информации, естественно возникает вопрос: «Что же представляет собой информация, получаемая и используемая при расследовании преступлений, каковы специфика, признаки, отличия, позволяющие отграничить ее от других видов социальной информации?».

В связи с тем, что в ходе расследования преступной деятельности субъект доказывания получает различную информацию из разных источников и с помощью различных средств, а принимает большинство юридически значимых решений лишь на основе доказательств, отдельными учеными [15, 90; 35, 33], и полагаем, вполне обоснованно производится разграничение информации на процессуальную (доказательственную) и непроцессуальную. Отграничение доказательственной информации и информации, полученной из непроцессуальных источников, по мнению Д. И. Беднякова, возможно только в результате рассмотрения таких основных категорий уголовного процесса, как доказательства, источники доказательств и средства доказывания [35, 33]. Такой способ определения понятия допускается в формальной логике в качестве вспомогательного наряду с другими правилами определения понятия, например, через ближайший род и видовое отличие [36, 409]. В данном случае для определения понятия (непроцессуальная информация) отыскивается ближайший род (информация о преступлении независимо от способов и источников ее получения), после чего выявляются признаки, характеризующие доказательственную информацию (доказательства), отсутствие которых позволяет определить (отграничить от доказательств) искомый вид. Такая формально-логическая операция называется дизъюнкцией (от латинского «disiunctio» — разобщение, разделение) [37, 98]. При этом два высказывания (определения) объединяются с помощью логического союза «или». В качестве примера можно привести следующее суждение: «информация о преступлении может быть или процессуальной (доказательственной) или непроцессуальной» [35, 34].

Думается, что критерием для разграничения доказательственной и непроцессуальной информации следует считать характеристику ее носителя и содержания. Однако указанными случаями разделение не ограничивается. Информация будет являться доказательственной, если она получена в порядке, установленном уголовно-процессуальным законом (то есть при производстве процессуальных действий с соблюдением норм их регламентирующих), а также, если обладает свойствами относимости и достоверности, критерии которых установ-

лены ст. 128 УПК РК. В иных случаях, полученная информация будет являться непроцессуальной.

Говоря о доказательственной информации, следует отметить, что центральным в теории доказательств является понятие доказательства. Отечественная доктрина, сформировавшаяся как результат многолетних исследований, рассматривает доказательство как аргумент, подтверждающий, обосновывающий существование факта, подлежащего доказыванию. Однако аргумент этот имеет свою форму (виды доказательств, различающиеся по способу сохранения и передачи содержащейся в них информации) и свое содержание (фактические данные). Первое определяет такое необходимое свойство доказательств, как их допустимость, второе — их относимость и достоверность.

Все положения норм УПК РК закрепляют и конкретизируют применительно к отдельным доказательствам конституционное положение о недопустимости доказательств, полученных с нарушением закона, подчеркивая этим неотделимость самого понятия доказательства от способа его получения. Сделан акцент на допустимость доказательств («доказательство считается допустимым, если оно получено в порядке, установленном настоящим кодексом» — ч. 4 ст. 128 УПК РК), в ущерб их относимости («доказательство признается относящимся к делу, если оно представляет собой фактические данные, которые подтверждают, опровергают или ставят под сомнение выводы о существовании обстоятельств, имеющих значение для дела» — ч. 3 ст. 128 УПК РК), в результате чего понятие доказательственной информации существенно обедняется.

Уголовно-процессуальный закон называет несколько случаев, когда информация, хотя и получена предусмотренными в законе способами, но в связи с несоблюдением процессуальной формы или условий производства процессуальных действий, не имеет доказательственного значения.

Первый случай обозначен в ст. 82 УПК РК и запрещает допрашивать в качестве свидетеля судью, защитника подозреваемого (обвиняемого) (представителя потерпевшего, гражданского истца, гражданского ответчика) об обстоятельствах дела, которые стали ему известны в связи с выполнением обязанностей по уголовному делу.

Второй закреплен в ст. 82 УПК РК и не позволяет допрашивать священнослужителя, об обстоятельствах, ставших известных ему на исповеди.

Третий предусмотрен в ст. ст. 82, 119 УПК РК и относится к показаниям лица, которое в силу своих физических или психических недостатков не способно правильно воспринимать обстоятельства, имеющие значение для дела, и давать о них правильные показания.

Четвертый указан в ч. 1 ст. 116 УПК РК для тех случаев, когда заключение по результатам исследования предметов, документов, материалов уголовного дела произведено некомпетентным лицом.

Пятый относится к получению процессуальной информации участниками уголовного процесса, подлежащими отводу (ст. 89 УПК РК).

Шестой сформулирован в ст. 123 УПК РК применительно к документам, которые, хотя и имеют значение для дела, тем не менее, не удостоверены пред-

приятиями, организациями, должностными лицами и гражданами. Это так называемые анонимные заявления и письма (в том числе и участников процесса), черновые записи, дневники, неофициальные бухгалтерские документы и так далее.

Несмотря на то, что информация, полученная названными способами и из перечисленных источников, не имеет доказательственного значения, полностью отказаться от ее использования нецелесообразно. Практика показывает, что информация, полученная без соблюдения требований уголовно-процессуальной формы (главным образом оперативно-розыскные данные), и сведения, содержащиеся в носителях, которые не могут стать (до определенного момента) источниками доказательств, успешно используются в расследовании преступлений и доказывании вины лиц их совершивших. Более того, между процессуальной и непроцессуальной информацией нет непреодолимой границы, так как она (непроцессуальная информация) при определенных в законе условиях может стать доказательственной (процессуальной), либо использоваться при принятии некоторых процессуальных, а также организационных и тактических решений.

Полагаем необходимым, остановить внимание еще на одном виде информации, вовлеченной в сферу уголовного процесса — иная процессуальная информация. Следует отметить, что здесь идет речь об информации, не имеющей доказательственного значения для расследования преступления. К такой информации, например, относятся, сведения, характеризующие личность обвиняемого, полученные из объяснений. Вторым примером иной процессуальной информации, является наличие в деле сведений, данных лицом, которое в силу своих психических недостатков не способно правильно воспринимать обстоятельства, имеющие значение для дела и в установленном кодексом порядке было признано неспособным на момент производства допроса (ч. 8 ст. 119 УПК РК). К иной информации также относятся фактические данные, которые были получены с нарушением требований Уголовно-процессуального кодекса и в соответствии ст. 116 УПК РК были признаны недопустимыми в качестве доказательств. Полагаем, что к данному виду информации могут относиться и сведения, закрепленные в протоколе разъяснения прав и обязанностей участника уголовного процесса, кроме тех случаев, когда нарушение возложенных на них требований, повлекло совершение преступления.

Подводя итог изложенному, на основе представленной классификации, и с учетом положений Уголовно-процессуального кодекса считаем, что вся информация по уголовному делу делится на процессуальную и непроцессуальную. Процессуальную информацию можно разделить на доказательственную и иную, непроцессуальную — на оперативно-розыскную информацию и иную.

Под доказательственной информацией следует понимать фактические данные истребованные, полученные, оформленные и закрепленные в порядке, установленном нормами Уголовно-процессуального кодекса органами уголовного преследования. То есть, к доказательственной относится информация, на основе которой устанавливаются обстоятельства дела, подлежащие доказыванию. Источниками получения доказательственной информации являются про-

токолы процессуальных, судебных действий и иные документы, полученные и представленные органу уголовного преследования в порядке, установленном ст. 125 УПК РК.

Под информацией, используемой в уголовно-процессуальной деятельности, следует понимать фактические данные (сведения) о лицах, предметах, фактах, событиях, явлениях и процессах охватываемых предметом доказывания и иных данных, относящихся к расследуемому делу. К информации, используемой в уголовно-процессуальной деятельности, относится и оперативно-розыскная информация.

Под оперативно-розыскной информацией понимается совокупность первичных и выводных данных о лицах, причастных (и подозреваемых) к подготовке и совершению преступлений, фактах преступных проявлений, состоянии оперативно-розыскных сил и средств, сведений, характеризующих оперативно-тактическую обстановку а также виды и способы совершения преступлений; приметы преступников, похищенных вещей; сведения о замышляемых и подготавливаемых преступлениях, об обстоятельствах, имеющих непосредственное или потенциальное значение для планирования и осуществления оперативно-розыскных мероприятий, проведения оперативно-аналитической работы, а также оказания содействия предварительному расследованию.

Информация должна быть представлена в форме удобной для использования, передачи, хранения и (или) обработки (преобразования) человеком или автоматизированными средствами. Целевое назначение информации применительно к раскрытию преступлений заключается в том, чтобы заранее определить круг лиц, среди которых может быть преступник, а также обеспечить обнаружение лиц, совершивших или совершающих конкретные преступления, получение доказательств их виновности.

Схематично, классификацию информации (на основании источников и порядка ее получения) в сфере уголовного судопроизводства можно представить следующим образом.

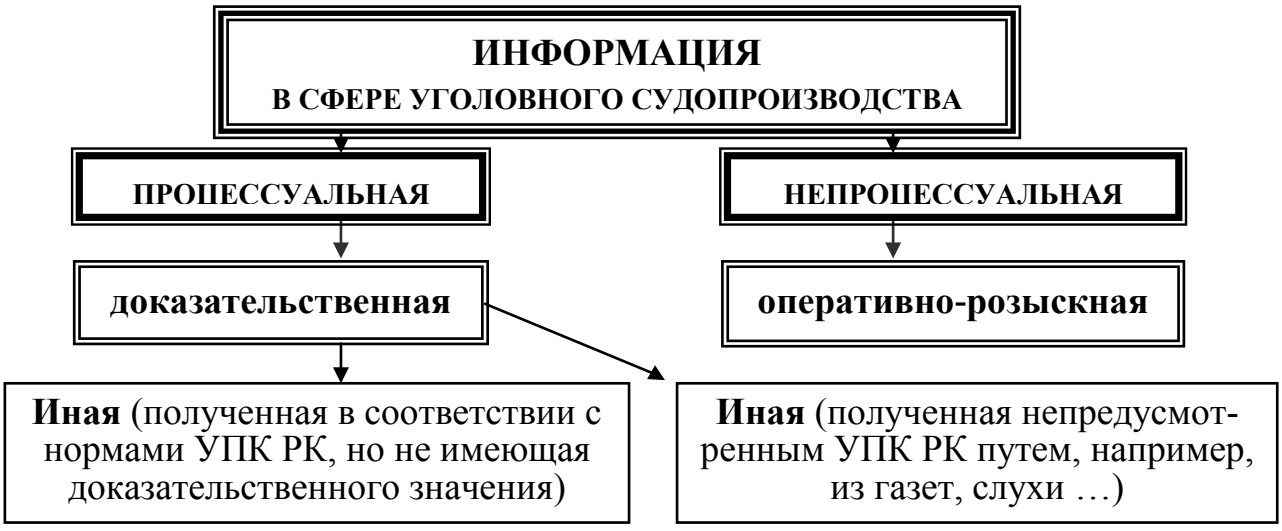

Рисунок 1 — Классификация информации в сфере уголовного судопроизводства

Разделение информации, используемой в уголовном процессе, на две вышеуказанные категории связано с тем, что оперативно-розыскная информация (хотя она и входит в процессуальную), может быть использована в доказывании по уголовным делам только при ее представлении в объеме и форме, позволяющих оценить содержащиеся в них фактические данные с точки зрения их относимости к расследуемому уголовному делу, допустимости, достоверности и в соответствии с требованиями, установленными нормами УПК (глава 21, ст. ст. 53, 100, 121, 123, 130, 202), а также Законом РК «О государственной защите лиц, участвующих в уголовном процессе» от 5 июля 2000 г. № 72-II.

При осуществлении расследования преступлений сотрудники полиции, осуществляющие операции над получаемой информацией (в том числе ограниченного доступа и личного характера), должны руководствоваться в своей деятельности принципами уважения и защиты человеческого достоинства по отношению ко всем лицам. И обязаны, в соответствии со ст. ст. 53, 205 УПК РК, предупредить участников проводимого действия о недопустимости разглашения ставших им известными сведений и ответственности за их разглашение без согласия следователя по ст. 355 УК РК.

Касаясь вопроса о видах информации, могущей быть вовлеченной в сферу уголовного процесса, предлагается объединенная классификация сведений (данных), имеющих обусловленное значение, сформированная на основе толкового [34, 55], юридического и энциклопедического словарей [4, 230; 5, 23-82] и других источников[35, 91; 38]:

- ***справочная информация*** — сведения или данные для выдачи справок о чем-то;
- ***сигнальная информация*** — предназначенная для быстрого предварительного оповещения;
- ***коммерческая информация*** — данные, сведения и содержащиеся в них документы, являющиеся объектом продажи их собственником;
- ***коммерческая тайна*** — 1) информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьи лицам, к ней свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности; 2) сведения о деятельности фирмы, предприятия, распространение которых наносит ущерб их интересам; 3) охраняемая законным владельцем информация о деятельности, направленной на получение прибыли, разглашение которой может принести ему вред;
- ***личная информация*** (информация персонального характера**)** — сведения о политических взглядах, философских, религиозных и других убеждениях, о принадлежности к политическим партиям, общественным движениям и ассоциациям, личной жизни, включая интимные ее стороны и сексуальное поведение, сведения о национальности, о состоянии физического и психического здоровья, о потреблении алкоголя и иных наркотических и токсических веществ, вкладах в сберегательном

банке, других видах собственности, а также сведения о погашенной судимости; сведения, данные о гражданах и организациях, затрагивающих их интересы и запрещенные для распространения без их согласия;

- ***библиографическая информация*** — библиографические данные, описания, их перечни;
- ***графическая информация*** — сведения или данные, представленные в виде схем, эскизов, изображений, графиков, диаграмм;
- ***ретроспективная информация*** — сведения, содержащиеся в накопленных за два и более лет массивах данных или полученные в результате поиска в этих массивах;
- ***документальная информация*** — сведения, закрепленные на каком-либо материальном носителе; содержание документа или текста;
- ***оперативная информация*** — сведения о чем-либо, наиболее быстро (в конкретных условиях) поступившие к пользователю; информация, полученная в результате осуществления ОРМ;
- ***информация с ограниченным доступом*** — предусмотренные законодательством сведения о человеке, обществе и государстве, предусматривающие специальный режим их сохранности и защиты от несанкционированного доступа или неправомерного обращения. По условиям ее правового режима подразделяется на информацию, отнесенную *к государственной тайне и конфиденциальную;*
- ***тайна государственная*** — защищаемые и специально охраняемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и ОРД, имеющие важное государственное значение, распространение которых может нанести ущерб безопасности государству. Служебная тайна является составной частью государственной тайны;
- ***конфиденциальная информация*** — сведения о личности, фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, которые охраняются законодательством в соответствии с правом гражданина на защиту от тайного надзора или нанесения ему ущерба со стороны государства, каких-либо юридических, а также других частных лиц. Конфиденциальная информация может содержать сведения, составляющие государственную, коммерческую, личную и другие виды тайны.

Изложенное позволяет утверждать, что в зависимости от вида, способа и условий получения информации, ее характера будут определяться порядок введения информации в процесс доказывания и специфика ее хранения и использования при расследовании преступлений. По характеру информацию можно разделить на компьютерную и иную. Природа информации определяет особенности работы с ней: обнаружение, исследование, фиксация изъятие и использование. Возникает вопрос и о носителях такой информации. Поэтому вопросы

получения информации с технических каналов связи и компьютерных систем и их значение в доказывании заслуживают самостоятельного исследования.

1.2 Понятие и виды документов как процессуальных источников информации, имеющей значение по делу

Согласно положениям ст. 236 УПК РК, сообщения и компьютерная информация, полученные в результате перехвата, фиксируются специалистом на соответствующем носителе и передаются следователю для использования в уголовном процессе и принятия процессуальных решений. Однако законодателем не указывается, можно ли представленный следователю носитель с информацией отнести к иным документам или предметам, имеющим значение для дела — вещественным доказательствам.

Анализируя положения Уголовно-процессуального кодекса Республики Казахстан мы видим, что термин «документ» используется практически во всех статьях и даже указывается некая разновидность документов — исполнительные, процессуальные, официальные и иные документы, документы которые могут иметь значение для установления обстоятельств по делу и тому подобные.

Но в тоже время следует отметить, что уголовно-процессуальным законодательством понятие «документа» не раскрывается. В ч. 1 ст. 123 УПК РК дается достаточно широкое и неконкретное определение документа — «… сведения, изложенные или удостоверенные, организациями, должностными лицами и гражданами …». А в ч. 2 ст. 123 УПК РК лишь отмечается, что «к документам могут относиться материалы доследственной проверки (объяснения и другие показания, акты инвентаризаций, ревизий, справки), а также материалы, содержащие компьютерную информацию, фото- и киносъемки, звуко- и видеозаписи, полученные, истребованные или представленные в порядке, предусмотренном статьей 125 настоящего Кодекса».

В связи с этим отдельные ученые, формируя словари понятий и терминов, используемых в уголовно-процессуальной и оперативно-розыскной деятельности, применяли выкладки и положения из других наук. В частности, в словаре основных уголовно-процессуальных понятий терминов [39, 34] в качестве основы для конструирования нормативного понятия «документ», использовали закрепленное ГОСТом 6.10.12-75 понятие, согласно которому: «Документ-это материальный объект, содержащий в зафиксированном виде информацию, оформленную в установленном порядке, имеющий в соответствии с действующим законодательством правовое значение». И на основе этого уголовно-процессуальные документы толковались как документы, в которых средствами письменной речи зафиксированы сведения, имеющие правовое значение и отражающие ход и результаты деятельности участников уголовного судопроизводства.

А. Ю. Шумилов, используя положения нескольких законов [40; 41], а также словарь современных терминов и понятий [42, 25], дает расширенное поня-

тие термина «документ» и полагает, что «документ (документированная информация), от латинского — свидетельство, доказательство»:

- носитель зафиксированной информации (в том числе и автоматизированный носитель информации);
- в информационно-поисковых системах — любой объект памяти (книга, чертеж и прочее);
- деловая бумага, юридически подтверждающая какой-либо факт и право на что-либо;
- зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

А также выделяет понятие оперативно-служебного документа как материального носителя с зафиксированной информацией (на бумаге, фото- и кинопленке, магнитной ленте и прочем), полученной в ОРД и оформленной по установленным в правоохранительных органах правилам делопроизводства [34, 21].

Обобщив указанные понятия можно предположить, что документ — это зафиксированная на материальном носителе и оформленная, в установленном порядке, информация с реквизитами, позволяющими ее идентифицировать.

Момент идентификации зафиксированной информации, как аспект, позволяющий считать ее документом, закреплен в Законе Республики Казахстан «О национальном архивном фонде и архивах» от 22 декабря 1998 г., регулирующим общественные отношения в области формирования, хранения и использования документов Национального архивного фонда Республики Казахстан и государственного управления архивным делом в Республике Казахстан. В статье 1 «Основные понятия, используемые в настоящем Законе» даны следующие основные понятия:

- документ — зафиксированная на материальном носителе информация, позволяющая ее идентифицировать;
- официальный документ — документ, созданный физическим или юридическим лицом, оформленный и удостоверенный в установленном порядке [43].

Приведенные примеры показывают, что определение термина «документ» является важным и необходимым для качественного ведения дел в различных сферах деятельности человека. Закрепление в уголовно-процессуальном законодательстве понятия «документ» позволит определить признаки и порядок приобщения к делу различной информации, имеющей значения для расследования преступлений и решения задач уголовного судопроизводства. В связи с чем, диссертантом предпринята попытка сформулировать понятие «документа» применительно к уголовно-процессуальному законодательству, а также предложена классификация документов с характеристикой каждого из них.

На основе приведенных выше положений Законов, ГОСТов, словарей, мнений ученых и иных источников [44, 23], предлагается следующее собственное определение документа: ***документ*** — материальный носитель, на котором условными знаками (буквами, цифрами и другими) зафиксирована информация о фактах, событиях, явлениях объективной действительности и мыслительной

деятельности человека, имеющая значение для дела, в том числе и информация, отражающая ход и результаты деятельности участников уголовного судопроизводства, с реквизитами, позволяющими ее идентифицировать. Документы могут подвергаться процессам записи (преобразования), хранения, поиска, передачи, получения, сбора и чтения. Отметим, что понятие материальный носитель является обобщающим наименованием материала, на который можно записывать данные.

Таким образом, исходя из приведенного понятия и в соответствии со ст. 123 УПК РК, выделяется два существенных признака, характеризующих документ. Во-первых, документ должен иметь вещественную основу (материальный носитель). Требование к материальному носителю — способность сохранять нанесенные на нём знаки. Способ нанесения знаков должен оставлять на предмете материальные следы, доступные к восприятию и прочтению. Знаки могут быть нанесены химическими средствами (тушью, чернилами, краской, мелом) либо механическими (изменение поверхности предмета резанием, штамповкой, гравировкой, выжиганием). Важно, чтобы знаки составляли логическую систему, передающую мысль.

Следует отметить, что содержание документов фиксируется на материальном носителе, который подразделяется на машиночитаемый и человекочитаемый.

Машиночитаемый носитель — носитель, пригодный для непосредственной записи и считывания данных техническими средствами (ЭВМ). Термин обычно применяется к устройствам внешней памяти (магнитные и оптические диски, дискеты и тому подобное). Однако он может использоваться и по отношению к определенной части твердых носителей, если они допускают использование специальных считывающих устройств (например, сканер).

Человекочитаемый (твердый) носитель — носитель, пригодный или используемый для записи данных, непосредственно считываемых человеком (например, бумага, фото-, кино- и фонодокументы).

Из изложенного следует, что документ представляет собой материальный носитель с зафиксированными на нём знаками, передающими мысль. Следовательно, для отнесения предмета к документу, не имеет значения материал, из которого он изготовлен (например, бумага или магнитофонная лента), способ его создания и каким условным кодом выражено его содержание. Таким образом, в сферу доказывания по уголовному делу могут быть вовлечены любые документы, поскольку документ, как материальный носитель информации, может фиксировать материальные следы преступления и существовать в сфере уголовного судопроизводства как самостоятельный вид доказательства и как вещественное доказательство. Так, И. Л. Петрухин, раскрывая содержание данных понятий, указывает: «документ становится вещественным доказательством в силу своей незаменимости, т. е. существует в единственном числе. А основным признаком документа как доказательства является наличие сведений, относящихся к расследуемому делу» [45, 191]. Следует дополнить, что сведения должны подтверждать, опровергать или ставить под сомнение выводы о суще-

ствовании обстоятельств, имеющих значение для дела, то есть обладать свойством относимости, и отметить, что документы как доказательства заменимы, поскольку могут быть воспроизведены их автором, а как прямые и косвенные доказательства могут являться первоначальными и производными, обвинительными и оправдательными.

Классифицируя документы, вовлеченные в процесс расследования, И. Л. Петрухин ставит в основу два основных признака документа. Первый — документ как доказательство, то есть наличие в нем сведений, относящихся к делу. Данный аспект был рассмотрен нами выше. И второй признак — наличие необходимых данных о субъекте, от которого исходит документ, разделяя на основе этого признака документы на официальные и частные. При этом, официальные документы трактуются им как документы, исходящие от организаций, предприятий, учреждений любой юридической природы и характеризуются наличием в них реквизитов. Реквизиты официальных должны удовлетворять всем требованиям, выполнение которых устраняет сомнение в их подлинности. Возникшие сомнения могут быть устранены посредством получения новых доказательств (например, при допросе). Говоря о частных документах, И. Л. Петрухин отмечает, что для них не установлено какой-либо обязательной нормы и акцентирует внимание на том, что в уголовном деле обязательно должны быть сведения об обстоятельствах появления документа (выемка, обыск, запрос, представление участником) [45, 192-193].

Думается, что представленная классификация требует некоторого уточнения, так как в уголовный процесс могут быть вовлечены материалы, не имеющие данных о субъекте, его предоставившем (например, анонимное сообщение, заявление, полученное при расследовании преступления). Отнести его к доказательствам мы тоже не можем, так как согласно п. 6 ч. 1 ст. 116 УПК РК — «... фактические данные должны быть признаны недопустимыми в качестве доказательств, если они получены от неизвестного источника либо от источника, который не может быть установлен в судебном заседании». Думается, что во втором случае наиболее применима категория «иных документов», вовлеченных в уголовный процесс.

Продолжая исследование категорий документов, используемых в уголовном процессе и анализируя положения Уголовно-процессуального кодекса, можно отметить, что закон фактически выделяет две группы документов, вовлеченных в процесс расследования. Первая — протоколы процессуальных действий (ст. 122 УПК РК), то есть зафиксированные данные, полученные при производстве процессуальных и судебных действий. Вторая — иные документы, полученные в ходе иной процессуальной деятельности (справки, акты, оперативно-розыскная информация и так далее). Где также ничего не говорится об отнесении анонимных сообщений к какой-либо категории документов.

Исходя из действующего уголовно-процессуального законодательства и порядка приобщения и вовлечения материалов в процесс расследования, следует констатировать тот факт, что в зависимости от формы, оформления, наличия

реквизитов и порядка их расположения, а также содержания, документы, используемые в уголовном судопроизводстве, можно разделить на два вида:

1. Процессуальные документы — документы, содержащие фактические данные, полученные в ходе следственных и судебных действий, оформленные и удостоверенные органами, ведущими уголовный процесс, в установленном Уголовно-процессуальным кодексом порядке, и имеющие в соответствии с действующим законодательством правовое значение.
2. Иные документы — разного рода документы, изготовленные как в ходе процессуальной деятельности, так и вне ее, но используемые в процессе как источники доказательств: материалы доследственной проверки, официальные и частные документы полученные, истребованные или представленные в порядке, предусмотренном ст. 125 УПК РК.

Говоря сегодня о различных видах документации (текстовой, изобразительной, фото-, кино-, видео-, фонодокументах), могущей быть вовлеченной в сферу доказывания, мы не можем не упомянуть об электронном документе, который «представляет собой интеграцию всех известных видов документов» [46, 122] и является неотъемлемой частью управленческой документации, основным источником информации в безбумажном учреждении будущего.

В связи с тем, что полученная при перехвате сообщений информация, копируется на машинный носитель, после чего по решению органа уголовного преследования может быть уничтожена, модифицирована, направлена адресату и (или) блокирована, то следует более подробно остановиться на видах документов, используемых при работе с ЭВМ.

Следует заметить, что если положение бумажных документов в жизнедеятельности человека определялось тысячелетиями, то история развития электронных документов, именно как документов, исчисляется лишь десятками лет. В связи с чем, существует нерешенность, в частности, вопросов электронного юридического атрибутирования документов, которая препятствует организации электронного документирования, документооборота, хранения и защиты информации от несанкционированного доступа. Поэтому, прежде чем заниматься технико-технологическими проблемами электронных документов, следовало решить терминологические проблемы, проблемы правового характера по отношению к машиночитаемым документам.

Нельзя сказать, что электронный документооборот — явление последних лет. Уже с середины 70-х годов велись разработка и принятие нормативных правовых актов, направленных на регулирование отношений в связи и по поводу электронных документов. Так, в 1980 г. Государственный комитет СССР по делам изобретений и открытий утвердил «Положение о всесоюзной магнитно-ленточной службе патентной информации» [47]. Но это в большей мере касалось внутриотраслевых электронных документов. 20 апреля 1981 г. Государственный комитет по науке и технике СССР утвердил «Временные общеотраслевые руководящие указания о придании юридическим документам, создаваемым средствами вычислительной техники» [48]. 9 октября 1984 г. Государ-

ственным комитетом СССР по стандартам был введен ГОСТ 6.10.4-84 «Придание юридической силы документам на машинном носителе и машинограммах, создаваемым средствами вычислительной техники». Но, по большому счету, в СССР электронный документооборот не получил широкого распространения в связи с существованием плановой экономики.

И только коренное изменение экономической и политической ситуации позволило ощутить актуальность вопроса электронного документа, так как сегодня речь идет не просто о внутриведомственном обмене информацией, а о построении бизнеса и развитии государства посредством электронных документов. Рассмотрению данного вопроса было посвящено множество дискуссий, в том числе и международного характера.

Так, 24-25 ноября 1999 г. была проведена VI Международная научно-практическая конференция: «Документ в информационном обществе». На конференции был обсужден комплекс вопросов по теме: «Электронное делопроизводство и электронный архив». Целью конференции явились постановка и обсуждение фундаментальных теоретических проблем, обобщение современной практики, выработка методических подходов и рекомендаций для поиска оптимальных решений научных и практических задач. В ходе конференции были рассмотрены вопросы, посвященные понятию электронного документа, законодательному обеспечению и правовым аспектам статуса электронной документации [49].

Можно вспомнить также и опыт Австралии, где впервые в мире в 1996 г. был принят Национальный стандарт по управлению документами, в котором содержатся рекомендации по работе с традиционными документами на бумажной основе и с современными электронными документами [50].

Итак, что же такое электронный документ, и какими характеристиками он обладает? Специфика машиночитаемых данных состоит в том, что мы не можем их воспринимать в том физическом виде, в каком они хранятся на носителе. Электронные документы очень сильно зависят от технологии, формата и стандарта, в рамках которых они создаются. Заметим, что данные, находящиеся в представляемом для ЭВМ виде, имеют материальный носитель (например, дискета). Основными видами носителей, применяемых при создании машиночитаемых документов, являются перфорационные (перфокарты, перфоленты) и магнитные (магнитные ленты, магнитные диски, карты с катушкой) носители записи. Данные нанесены в виде специальных знаков (двоичного кода), расположенных в соответствии со специальным алгоритмом (то есть упорядоченно, системно). Только пройдя через ряд предусмотренных процедур, данные предстают в понятном пользователю виде (в распечатанном виде, на экране монитора и тому подобном). Отсюда и терминологические разногласия, наблюдаемые как в среде ученых, так и в среде специалистов и практиков.

В одном случае под электронным документом понимается машинный носитель информации, в другом — отдельный файл на этом носителе, в третьем — распечатка на бумаге, в четвертом — некая «матрица в памяти компьютера» [51].

Во многих случаях за документ принимается изображение на экране, в том числе полученное по электронной почте, из Интернета и других сетей. Не следует упускать из виду, что в рассматриваемом термине имеет значение не только первое слово «электронный», но и «документ». Понятие документа уже достаточно определено и, несмотря на варианты, имеет ряд общих обязательных составляющих: закрепление информации на носителе, возможность сохранения и передачи во времени и на расстояние, возможность служить доказательством.

Так, в толковом словаре по информатике под редакцией Ф. С. Воройского, даны следующие виды машинных документов:

- документ на машиночитаемом носителе — документ, созданный средствами вычислительной техники, записанный на машиночитаемый носитель, оформленный в установленном порядке и пригодный для автоматического считывания содержащейся в нем информации;
- электронный документ, электронный текст — совокупность данных в памяти вычислительной системы, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств [44, 25].

Нельзя не привести определение электронного документа, указанного в проекте Закона «Об электронно-цифровой подписи» в редакции от 15 мая 2000 г., подготовленного коллективом авторов под эгидой Минсвязи: «Документ в электронной форме отображения (электронный документ) — информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущая быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющей атрибуты идентификации документа» [52].

В тоже время, по мнению главного специалиста Депозитария АКБ РОСБАНК Н. Соловьева «электронный документ может объединять в себе несколько пересылаемых файлов, а приложением к нему будет являться протокол, содержащий указание о том, кому он предназначен и, возможно, некоторую дополнительную служебную информацию. Каждый электронный документ обязательно имеет электронную подпись отправителя. Каждый файл, входящий в электронный документ, может иметь, а может и не иметь электронной подписи, в том числе может иметь несколько электронных подписей и не обязательно отправителя» [53].

Дополняя рассматриваемый аспект, отметим, что Госдума РФ приняла закон об электронно-цифровой подписи. Документы с такой подписью будут иметь те же права, что и традиционные бумажные, при выполнении следующих условий:

- сертификат на момент подписания действителен;
- электронная подпись проверена открытым ключом;
- файл после подписания не изменялся;

– а если некое лицо воспользуется чужой подписью или неправомерно раздобудет закрытый ключ, то оно понесет уголовную, гражданско-правовую или административную ответственность [54, 98].

Исследуя техническую сторону состояния электронного документа, следует отметить, что:

– каждый электронный документ включает в себя файл-реестр VTELEDOC.RE (если документ не шифрованный) или VTELEDOC.CRE (если документ шифрованный) с перечнем файлов, вошедших в документ. В реестре для каждого файла указывается его имя и информация о том, является ли он подписанным или нет;
– каждый файл с электронным документом имеет имя «*.D», где «*» — первые восемь символов его электронной подписи;
– каждый электронный документ перед отправлением может быть зашифрован и его содержание будет доступно только конечному получателю, но недоступно администраторам, при этом подписываться будет уже зашифрованный документ. Отметим, что шифруется уже готовый документ, содержащий файлы в архивированном виде;
– к каждому электронному документу прилагается по крайней мере один протокол, имя файла с протоколом имеет вид «*.Pnn», где «*» — упоминавшиеся выше первые восемь символов электронной подписи документа, P — фиксированный символ (признак протокола), nn — порядковый номер протокола в 16-ричной записи. К одному электронному документу может быть приложено несколько протоколов (случай циркулярной рассылки документа).

Заслуживает внимания Закон Туркменистана об «Электронном документе», в котором закреплены основные требования, предъявляемые к электронным документам, установлены правовые основы использования электронных документов. В ст. 1 «Понятие электронного документа» указано, что под электронным документом понимается информация, зафиксированная на машинном носителе, заверенная электронной цифровой подписью в соответствии с процедурой создания такой подписи. Кроме того, согласно ст. 5 данного Закона, электронный документ должен соответствовать следующим требованиям:

– создаваться, обрабатываться, храниться, передаваться и приниматься с помощью программных и технических средств;
– содержать реквизиты, позволяющие подтвердить его подлинность и целостность;
– быть отображенным (воспроизведенным) в форме, понятной для восприятия человеком [55].

Кроме рассмотренных выше понятий, законодательством Казахстана были введены другие понятия документов, созданных или используемых при помощи ЭВМ. В частности, постановлением Кабинета Министров Республики Казахстан «Об утверждении Основных правил документирования и управления

документацией в объединениях (предприятиях), учреждениях и организациях всех организационно-правовых форм Республики Казахстан» было закреплено:

- машиночитаемый текст — документ на машинном носителе;
- машиночитаемый документ — документ, пригодный для автоматического считывания содержащейся в нем информации;
- машинограммы — документ на бумажном носителе, созданный средствами вычислительной техники в письменной форме и оформленный в установленном порядке [56]. С 26 февраля 2003 г. данное постановление утратило силу, так как принятый Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» дает обобщающее определение различных видов машинных документов, объединив их понятием электронный документ — «документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи» [57].

Такая множественность понятий электронного документа еще раз подтверждает актуальность определения данного термина. В связи с тем, что закрепление в уголовно-процессуальном законодательстве понятия «электронный документ» и его видов позволит определить признаки и порядок приобщения к делу различной информации, имеющей значения для расследования преступлений, предлагается, на основе анализа приведенных источников, учитывая положения Законов, ГОСТов, словарей, мнений ученых следующее понятие электронного документа:

Электронный документ (машиночитаемый документ) — совокупность данных, оформленная в установленном порядке и представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, зафиксированная на машиночитаемом носителе, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств и имеющая атрибуты идентификации документа.

В качестве требований, предъявляемых к электронным документам, предлагается исходить из того, что электронный документ должен создаваться, обрабатываться, храниться, передаваться и приниматься с помощью программных и технических средств; содержать реквизиты, позволяющие подтвердить его подлинность и целостность; быть отображенным (воспроизведенным) в форме, понятной для восприятия человеком.

Электронный документ может объединять в себе несколько пересылаемых файлов и тогда он включает в себя файл-реестр с перечнем файлов, вошедших в документ. Каждый файл, входящий в электронный документ, может иметь одну или несколько электронных подписей и не обязательно отправителя. В реестре для каждого файла указывается его имя и информация о том, является ли он подписанным или нет. Приложением к такому документу будет являться протокол, содержащий указание о том, кому он предназначен и, возможно, некоторую дополнительную служебную информацию. К одному электронному документу может быть приложено несколько протоколов.

Каждый электронный документ перед отправлением может быть зашифрован, при этом подписываться будет уже зашифрованный документ.

Рассматривая вопрос о необходимости введения реквизитов для электронного документа, полагаем, что проверка наличия и соответствия реквизитов в электронном документе позволит сотрудникам правоохранительных органов, при исследовании таких документов, выявлять наличие подделки, подлога, автора и времени создания документа и других, имеющих значение обстоятельств. Интересно в связи с этим отметить, что популярный текстовой редактор «Microsoft Word» создает текстовые документы, формат которых предусматривает автоматическое сохранение в них сведений о дате создания и последнего изменения файла, об авторе, об организации, которая использует конкретный экземпляр программы «Microsoft Word», имени руководителя, названии темы документа в файле, общем времени работы с файлом, и других данных. При этом файл может быть защищён паролем.

Кроме того, по мнению отдельных авторов, наличие в электронном документе необходимых реквизитов (наименование организации, имя создателя документа, местонахождение организации, дата изготовления документа, код лица, ответственного за изготовление документа, код лица, утвердившего документ) позволит придать ему юридическую силу [58, 98; 59, 253].

В связи с чем, считаем необходимым для электронных документов и машинограмм применять требования, указанные в «Методических указаниях по приданию юридической силы документам на машинном носителе и машинограммам, создаваемым средствами вычислительной техники», в которых установлен комплекс обязательных реквизитов и порядок их расположения, а также указано, что «подлинники, копии машиночитаемых документов имеют одинаковую юридическую силу. Подлинником является первая по времени запись на машинном носителе; копией — документ, переписанный с подлинника и аутентичный по содержанию».

Полагаем, что в состав обязательных реквизитов электронного документа должны входить:

- код и наименование организации создателя документа (код и наименование записываются по классификатору предприятий и организаций);
- местонахождение организации — создателя документа или почтовый адрес (данный реквизит должен быть записан в следующем виде: код населенного пункта, в соответствии с классификатором обозначений объектов административно-территориального деления и наименование населенного пункта);
- код формы и название документа (записываются по действующим классификаторам управленческой документации);
- дата изготовления документа;
- код лица, ответственного за правильность изготовления документа, который записывается в следующем виде: код, должность, фамилия лица, ответственного за правильность изготовления документа или лица,

утвердившего документ (принадлежность кода конкретному лицу должна быть зарегистрирована в организации — создателе документа).

При создании дубликатов и копий машиночитаемых документов машинограмм в состав реквизитов включается отметка о подлинности документа (подлинник, копия). Дополнительные реквизиты применяются по решению министерств и ведомств (например, могут быть указаны номер телефона, телетайпа, должность и фамилия лица, имеющего право удостоверять машиночитаемый документ). Изменение подлинника может производить только организация-создатель документа; изменения в копии вносятся на основании извещения об изменениях.

Между тем, следует констатировать, что производство по делам, в которых в качестве доказательств фигурируют электронные документы, не получило должной регламентации в процессуальном законодательстве и юридической науке. Имеющаяся ссылка в ч. 2 ст. 123 УПК РК на использовании в процессе расследования компьютерной информации не раскрывает всех особенностей использования электронных документов в процессе расследования. В связи с чем, полагаем необходимым в рамках настоящего исследования изложить доводы, определяющие возможность участия электронного документа в процессе доказывания.

Так, в теории уголовного процесса под документом понимается любое письменное доказательство, в том числе сведения, зафиксированные с помощью различных приспособлений, аппаратов, машин [60]. Применение научно-технических средств в процессе доказывания закреплено в ст. 129 УПК РК, согласно которой «в целях собирания, исследования и оценки доказательств орган, ведущий уголовный процесс, вправе использовать научно-технические средства», если они «прямо предусмотрены законом или не противоречат его нормам и принципам, научно состоятельны, обеспечивают эффективность производства по уголовному делу». Таким образом, получение и закрепление с помощью электронно-вычислительной техники машиночитаемых документов и вовлечение в сферу уголовного процесса вполне обоснованно и актуально. Об этом также свидетельствует Приказ Министерства внутренних дел Республики Казахстан «О повышении эффективности применения научно-технических методов и средств в борьбе с преступностью» [61].

Кроме того, в гражданском процессе документ рассматривается как разновидность письменных доказательств, что не противоречит способности электронного документа быть воспринятым человеком и содержать в себе информацию, имеющую значение для дела [62, 430]. Электронный документ в отличие от бумажного представляет собой определенные данные, записанные на компьютерных носителях, обладающих определенными физическими характеристиками. Именно физические характеристики — вот что отличает два типа вышеуказанных документов. Если бумажный документ мы можем осязать, если на бумаге можно поставить подпись и печать, если сама бумага может быть защищена какими-либо специальными знаками (например, водными), то к электронному документу все эти характеристики неприменимы. Хотя все остальные

требования, предъявляемые к документам, аналогичны для обоих видов: содержание сведений определенного характера; изложение данных в установленных порядке и форме; содержание всех необходимых данных о сторонах, допустим, договора и так далее.

В пользу участия электронного документа в расследовании служит и то, что он может быть отнесен к делу точно так, как и любые другие данные. Следовательно, он может использоваться при решении тактико-организационных задач. Однако для того, чтобы служить доказательством по уголовному делу, фактические данные (электронная информация) должны обрести еще и свойство допустимости. Они должны быть получены:

- надлежащим субъектом доказывания;
- надлежащим способом собирания доказательств;
- из известного источника доказательств.

Полагаем необходимым рассмотреть два последних элемента допустимости доказательств, применительно к электронной информации.

Так, К. Б. Калиновский и Т. Ю. Маркелова, исследуя данный аспект, полагают, что для уголовно-процессуального использования электронная информация должна получить свое закрепление на каком-либо носителе. Электронная информация может найти свое отражение на фотоснимке, видеозаписи (с экрана компьютера), в памяти человека очевидца. Разумеется, электронные данные могут быть записаны на магнитный носитель или напечатаны на бумаге. В то же время электронная информация может быть сразу зафиксирована в уголовно-процессуальном порядке в протоколе следственного действия. Например, в ходе осмотра. Она может быть непосредственно занесена в протокол осмотра, а также дополнительно зафиксирована в приложениях к нему в результате фотосъемки или видеозаписи. Фиксация в протоколе следственного действия электронной информации возможна, как правило, без помощи специалиста и целесообразна, когда не требуется экспертное исследование [63, 18-19].

Однако нередки случаи, когда следователь иметь дело с носителями электронной информации, полученными вне уголовно-процессуальных действий. В этом случае он должен собрать носители данных путем производства следственных действий, истребования или принятия представленных предметов или документов.

После процессуального собирания носителей электронной информации они могут стать источниками доказательств определенного вида при соблюдении требований, к ним предъявляемых, в том числе при известности источника. В результате выемки, осмотра, обыска, истребования или принятия носитель информации может стать либо иным документом, либо вещественным доказательством. Вопрос об отграничении документов — вещественных доказательств от иных документов является самостоятельной научной проблемой. Для того чтобы электронный или бумажный документ признать вещественным доказательством, на наш взгляд, необходимо выполнение двух условий.

Во-первых, зафиксированная в документе информация должна содержать сведения о преступлении, а также об обстоятельствах, имеющих значение для

раскрытия и расследования, которые могут включать: причины и условия, способствовавшие совершению преступления, размер ущерба, подлежащего возмещению и иные элементы предмета доказывания.

Во-вторых, возникновение самого документа должно быть связано с преступлением, с его подготовкой, совершением или сокрытием.

Другими словами, вся информация в документах должна быть результатом человеческой деятельности. Например, сообщение об акте терроризма, размещенное в Интернете, будучи приобщенным к уголовному делу в виде распечатки, магнитного носителя, фотографии или видеозаписи, станет вещественным доказательством.

В практике бывает недостаточно двух вышеназванных критериев для отграничения документов от вещественных доказательств. Поэтому неустранимые сомнения трактуются в пользу вещественного доказательства, имеющего более строгую процессуальную форму.

Важно отметить, что первоисточником вещественного доказательства является сам предмет, отразивший искомое событие (например, факт сообщения об акте терроризма). Следователь для решения вопроса о допустимости электронного документа в качестве вещественного доказательства обязательно должен знать автора документа. Известность автора — это минимальное требование к документу. Например, в качестве доказательства следует рассматривать полученное сообщение по электронной почте очевидца угона автомашины в ответ на помещенное объявление потерпевшего о розыске очевидцев.

Для электронных документов серьезной юридической и технической проблемой является их удостоверение. Существующие в настоящий момент электронные подписи и другие возможности идентификации лиц, например в банковских компьютерных сетях, могут быть использованы и в уголовном процессе. Однако основным способом удостоверения в настоящее время, в силу недостаточной технической оснащенности территориальных органов полиции, остается установление автора документа с помощью других доказательств, например, путем его допроса. Следует отметить также большую роль специальных познаний в установлении причинной связи электронных следов с обстоятельствами, входящими в предмет доказывания. Данный аспект более детально будет рассмотрен нами в следующих главах диссертации.

Сказанное позволяет сделать вывод, что «электронный документ» может рассматриваться как разновидность документов и быть вовлеченным в сферу уголовного судопроизводства в качестве вещественного доказательства или иного документа. Данное высказывание подтверждается положением ст. 7 Закона РК «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. № 370-II, согласно которой «электронный документ, соответствующий требованиям настоящего Закона, равнозначен документу на бумажном носителе» [57].

Таким образом, технические каналы связи, как источники доказательственной информации, содержат информацию, закрепленную в знаковой и сигнальной форме. Процессуальной формой закрепления данной информации яв-

ляется документ, который обладает спецификой, отражающей природу информации. На основании вышеизложенного, анализа приведенных источников, учитывая положения законов, ГОСТов, словарей, мнений ученых в целях совершенствования уголовно-процессуального законодательства Республики Казахстан предлагается при работе с документацией использовать следующую терминологию:

Компьютерная информация — информация, зафиксированная на машинном, магнитном носителе, представленная в форме набора состояний элементов ЭВМ, иных электронных средств обработки, хранения и передачи информации. Компьютерная информация может являться подлинником или копией. Подлинник — первая по времени запись на машинном носителе; копия — более поздняя запись, аутентичная по содержанию, переписанная с подлинника. Изменение подлинника может производить только лицо или организация — создатель документа; изменения в копии вносятся на основании извещения об изменениях.

Компьютерная информация может иметь типичные и факультативные свойства, которые с криминалистической точки зрения могут быть использованы для идентификации файла и находящейся в нем информации, что имеет важное значение при расследовании компьютерных преступлений.

К типичным свойствам относятся:

1) наименование файла (включая его местоположение на диске — «путь»);
2) размер файла;
3) время создания, модификации;
4) системные атрибуты («системный», «только для чтения» и другие);
5) тип информации, хранящейся в файле (текстовая, графическая и так далее);
6) машинный носитель, его тип, номер, метка и другие.

К факультативным свойствам относятся:

1) программные средства, с использованием которых был создан или модифицирован файл (использование специальных символов, выделений, отметок в коде программы или документе, указателей на версию, серийный номер программного продукта, зарегистрированный пользователь программного продукта и другое);
2) автор, создавший или модифицирующий файл (программу в целом);
3) группа файлов (программные средства, группы документов), куда включен файл (в качестве отдельного документа или части программного кода);
4) ключевые слова, заметки автора или редактора и тому подобное.

Приведенные выше свойства, при отражении их в протоколах следственных действий, позволят удостоверить относимость, допустимость и достоверность полученной информации, при ее дальнейшем использовании в качестве доказательства при расследовании уголовных дел.

Машинограмма — документ на бумажном носителе, созданный средствами вычислительной техники в письменной форме и оформленный в установленном порядке. На машинограммах, представляющих особо важную информацию, подпись удостоверяется печатью организации — создателя документа.

Материальный носитель — обобщающее наименование материала, на который можно записывать данные. Носители подразделяются на: машиночитаемый носитель — пригодный для непосредственной записи и считывания данных техническими средствами (ЭВМ) — магнитные и оптические диски, дискеты и тому подобное; человекочитаемый (твердый) носитель — пригодный или используемый для записи данных, непосредственно считываемых человеком — бумага, фото-, кино-, фонодокументы и другое.

Электронный документ (машиночитаемый документ) — совокупность данных, оформленная в установленном порядке и представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, зафиксированная на машиночитаемом носителе, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств и имеющая атрибуты идентификации документа.

Электронный документ может рассматриваться, как полноценный документ, и быть вовлечен в сферу уголовного судопроизводства как вещественное доказательство или иной документ. Он должен:

- создаваться, обрабатываться, храниться, передаваться и приниматься с помощью программных и технических средств;
- содержать реквизиты, позволяющие подтвердить его подлинность и целостность;
- быть отображенным (воспроизведенным) в форме, понятной для восприятия человеком.

Электронный документ может объединять в себе несколько пересылаемых файлов. Каждый файл, входящий в электронный документ, может иметь одну или несколько электронных подписей и не обязательно отправителя. Данный вид электронного документа должен включать в себя файл-реестр с перечнем файлов, вошедших в документ. В реестре для каждого файла указывается его имя и информация о том, является ли он подписанным или нет. Приложением к такому электронному документу будет являться протокол, содержащий указание о том, кому он предназначен и, возможно, некоторую дополнительную служебную информацию. Любой электронный документ или компьютерная информация могут быть зашифрованы.

Документ — материальный носитель, на котором условными знаками (буквами, цифрами и другими) зафиксирована информация о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека, имеющая значение для дела, в том числе и информация, отражающая ход и результаты деятельности участников уголовного судопроизводства, с реквизитами, позволяющими ее идентифицировать.

Процессуальные документы — фактические данные, полученные в ходе следственных и судебных действий, оформленные и удостоверенные органами, ведущими уголовный процесс в установленном Уголовно-процессуальным кодексом порядке, и имеющие в соответствии с действующим законодательством правовое значение.

Иные документы — разного рода документы, изготовленные как в ходе процессуальной деятельности, так и вне ее, но используемые в процессе как источники доказательств: материалы доследственной проверки; *официальные и частные* документы полученные, истребованные или представленные в порядке, предусмотренном ст. 125 УПК РК.

Официальные документы — документы, электронные документы, созданные физическим или юридическим лицом, оформленные и удостоверенные в установленном порядке, имеющие в соответствии с действующим законодательством правовое значение. Официальные документы, исходящие или выдаваемые организациями, предприятиями, учреждениями любой юридической природы, характеризуются наличием в них реквизитов. Реквизитами являются бланк документа, его форма, цвет, размер, наличие защитных средств, оттисков печатей и штампов, фотокарточки, подписи должностных лиц.

Частные документы — документы, созданные физическим лицом, не имеющие какой-либо обязательной нормы и реквизитов (частные записки, личные письма и другие).

1.3 Компьютерные системы и технические каналы связи как объект уголовно-процессуальных действий

С появлением компьютерных сетей Земля все больше стала напоминать «всепланетный поселок» по выражению канадского социолога Маршалла Маклугана [33, 90]. Стремительное развитие информационных технологий приводит к тому, что многие явления социальной жизни все в большей мере находят отражение в так называемых «виртуальных мирах». Развитие глобальных компьютерных телекоммуникаций изменяет проведение деловых встреч, способы общения между людьми — с каждым месяцем увеличивается электронный документооборот в сетях Интернета — деловые бумаги, контракты, письма, дружеские сообщения, поздравительные открытки и масса иной информации вращается в электронных сетях.

В силу того, что организованная преступность в настоящее время использует средства компьютерных телекоммуникаций при подготовке к совершению преступлений как средство связи, средство криминальной переброски финансовых средств, компьютерные системы являются важным источником получения информации при расследовании преступлений, и в частности — объектом такого следственного действия как перехват сообщений.

В настоящее время одной из задач правоохранительных органов становится отслеживание криминальных явлений в сети «Интернет». Такая работа ведется за рубежом, в частности в США (ФБР) и в Германии (ВКА), где созданы

специальные подразделения компьютерной разведки в сети «Интеренет», осуществляющие поиск злоумышленников и адресатов, распространяющих криминальную информацию в компьютерных сетях [15, 324-326].

Насколько это направление деятельности правоохранительных органов является перспективным, говорит международное совещание экспертов в Японии в сентябре 1998 г., на котором, в частности, обсуждался вопрос о правовых основах и методике организации обыска компьютерных систем без изъятия компьютеров, а с помощью удаленного доступа, то есть с применением методов и средств сетевой компьютерной разведки. В правовом отношении компьютерную разведку можно рассматривать в качестве разновидности таких мероприятий, как снятие информации с технических каналов связи, наблюдение, исследование предметов и документов, оперативный осмотр.

Широкое использование для обработки информации локальных и глобальных вычислительных сетей делает чрезвычайно перспективным разработку соответствующих методов получения информации. Проблема получения и использования компьютерной информации представляется чрезвычайно актуальной и для Республики Казахстан. Это подтверждается введением в уголовно-процессуальное законодательство нового следственного действия — «Перехват сообщений», закрепленного в ст. 236 УПК РК. В статье, кроме регламентации оснований и порядка производства перехвата сообщений, передаваемых по техническим и компьютерным каналам связи, включено и производство дополнительного действия — снятие информации с компьютерных систем.

Между тем, введение уголовно-процессуальных новшеств требует активного научного исследования нормы, связанной с получением и использованием информации, полученной при производстве перехвата сообщений и порождает ряд вопросов. Так, законодателем не определены понятия таких основных терминов как: компьютерные и технические каналы связи, компьютерная система, снятие информации, разъяснение содержания которых позволило бы определить пределы вторжения сотрудников правоохранительных органов в базы данных физических и юридических лиц, способы получения необходимой информации и ее сортировки.

Слово «компьютер» нами воспринимается как нечто придуманное современниками. А в действительности оно пришло к нам из далекой древности. Словом «computare» латиняне обозначали понятие «считать», «вычислять». И только совсем недавно, 50-60 лет назад, понятие «компьютер» стало ассоциироваться со сложной машиной, техникой [64, 63]. В различной литературе, в том числе и специальной, данное понятие трактуется по-разному — «компьютер», «персональный компьютер», «ЭВМ». Если в общеразговорной речи людей различие в обозначении компьютера разными терминами не несет каких-либо последствий, то в правовом аспекте трактовка вышеуказанных понятий имеет немаловажной значение. В частности, в процессуальном праве определение и соотношение понятий «компьютер», «персональный компьютер», «ЭВМ», при их указании в процессуальных документах влияет на установление количества компонентов, подлежащих описанию (изъятию), выявление особен-

ностей функционирования компьютера (является ли он сервером, включен ли в компьютерную сеть, к каким адресатам имеет доступ и тому подобное) при производстве осмотра, обыска, опознания и других следственных действиях, а также на тактику их производства. Существует несколько точек зрения по содержанию термина «компьютер».

Так, под компьютером понимается аппаратно-программная реализация вычислительного устройства, обеспечивающая сбор, накопление, обработку и выдачу информации [33, 90]. В. В. Крылов считает, что компьютер это то же, что и электронно-вычислительная машина (ЭВМ), являющее собой комплекс электронных устройств, позволяющих производить предписанные программой и пользователем операции над символьной и образной информацией [65, 190]. Такой же точки зрения придерживается Б. Х. Толеубекова, которая, между тем, выделяет и такое понятие персонального компьютера (ПК) — компьютер индивидуального пользования, позволяющий применять типовые вычислительные программы и через телефонный канал выходить в информационно-вычислительную сеть, а также к источникам массовой информации [64, 65]. По мнению же С. Симоновича, персональный компьютер — это электронный прибор, предназначенный для автоматизации, хранения, обработки и передачи информации [66, 463].

Все выше обозначенные высказывания, несмотря на разную трактовку, сходятся в том, что компьютер является электронным устройством, позволяющим производить различные операции над информацией. Таким образом, можно с уверенностью считать, что понятия «компьютер», «персональный компьютер», «ЭВМ» являются синонимами, что также подтверждается толкованием понятия «компьютер» в современном словаре иностранных слов — компьютер англ. — «computer» производное от латинского «computare» — считать, вычислять; то же, что ЭВМ [67, 462].

Вместе с тем, указанные трактовки не отражают интересующего нас процессуального аспекта, касающегося компонентов ПК, а лишь отражают его общее назначение. Полагаем, что трактовку понятия «компьютер», необходимо дополнить содержанием об устройстве компьютера. Используя также работу В. Э. Фигурнова [68, 156] об устройствах, входящих в ПК, в совокупности с обозначенными выше трактовками, предлагается понятие «компьютера», применимого к уголовно-процессуальной деятельности.

Так, под компьютером (персональным компьютером (ПК), ЭВМ) следует понимать 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, джойстик, мышь, световое перо, микрофон, факс-модем, стример, сканер, плоттер и другое).

При производстве следственных действий к компьютеру (помимо основных частей — системный блок, клавиатура, монитор) будут относиться и другие устройства, встроенные в системный блок (например, модем), монитор (видеокамера) и клавиатуру (телефон, джойстик). При описании дополнительных устройств (например, принтер, сканер), в протоколах следственных действий следует указывать, что «… кроме компьютера (марка, тип, модель), состоящего из системного блока, монитора, клавиатуры (указать другие встроенные устройства, если подключены), в комнате находится принтер (модель, тип), который на момент проведения следственного действия к компьютеру не подключен ...». Дополнительные устройства подлежат исследованию как отдельные объекты, но в последующем (например, при производстве следственного эксперимента) могут быть подключены к компьютеру с целью установления возможности их функционирования и раннего использования на данной ЭВМ. Данный вывод подтверждается и практическими примерами. Так, при расследовании уголовного дела по факту изготовления и сбыта поддельных денег, при производстве обыска у Л. был изъят сканер, с помощью которого он вместе с А. изготавливал поддельные деньги. При производстве следственного эксперимента, сканер был подключен к компьютеру, изъятому у А., и в процессе исследования информационного содержания ПК были обнаружены файлы с изображением банкнот достоинством 200 и 500 тенге и программное обеспечение на сканер с установками на данную модель [69].

Следует отметить, что компьютерная информация зачастую хранится и обрабатывается лишь в памяти конкретной ЭВМ и вообще не попадает в каналы связи. Складывается ситуация, при которой информационные массивы, используемые в преступной деятельности и способные помочь раскрытию преступлений, остаются недоступными для правоохранительных органов при применении традиционных видов технической разведки. В то же время, по мнению отдельных ученых, имеется техническая возможность, активно воздействуя на компьютерные средства на уровне операционной системы, принудительно вызвать выдачу интересующей информации в канал связи.

«Во-первых, практически, на компьютерную систему в процессе ее исследования можно, осуществить воздействие с помощью технических средств, обеспечивающих появление информации в техническом канале связи.

Во-вторых, в последующем снять эту информацию с технического канала связи для использования при расследовании преступлений» [70, 386].

Основными факторами, определяющими особенности доступа к информации, являются как аппаратно-программная платформа, так и степень интеграции ее элементов. По степени интеграции можно выделить следующие типы вычислительных систем: отдельная вычислительная машина (компьютер), локальная компьютерная сеть, глобальная компьютерная сеть.

Говоря о снятии информации с компьютерных систем необходимо раскрыть понятие «компьютерная система» и виды систем, действующих в «электронном мире». Анализируя различные трактовки понятия «система», под которыми понимается: «определенный порядок в расположении и связи частей

чего-нибудь; форма организации чего-нибудь; нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей» [4, 661]; «(греч. Systema) целое, составленное из частей, соединений; — множество закономерно связанных друг с другом элементов (предметов), представляющее собой определенное целостное образование, единство» [67, 562], мы видим, что во всех случаях система трактуется как нечто целое, состоящее из различных элементов, взаимодействующих друг с другом. В то же время, Ф. С. Воройский дает расширенное толкование данного понятия и полагает, что «система, в широком значении термина — образующая единое целое совокупность материальных и (или) нематериальных объектов, объединенная некоторыми общими признаками, свойствами, назначением или условиями существования, жизнедеятельности, функционирования и т. п., а по отношению к техническим системам — взаимосвязанная общим управлением, назначением или условиями функционирования совокупность различных объектов и отношений между ними, образующая единое целое» [44, 247-248].

Таким образом, применяя по аналогии понятие «системы» для формирования трактовки понятия «компьютерная система» можно согласиться с мнением Ю. М. Батурина и А. М. Жодзишского, что компьютерная система — это любая система, в состав которой входит компьютер, предназначенный для управления этой системой либо для принятия решений [33, 90].

Однако С. Симонович, Г. Евсеев вполне обоснованно полагают, что наличие компьютера в какой-либо системе не характеризует ее как компьютерную, и считают, что «компьютерная система — совокупность аппаратного и программного обеспечения, действующего совместно», отмечая, что как аппаратное, так и программное обеспечение, являются необходимым элементом компьютерной системы. Под аппаратным обеспечением ими понимается совокупность технических устройств и приборов, а программное обеспечение — это совокупное название программных и информационных ресурсов (данных), используемых в работе с компьютером [66, 454].

Такого же мнения придерживается и Ф. С. Воройский, в то же время дополняя, что «computer system — вычислительная система — это также любая автоматизированная система, основанная на использовании ЭВМ и представляющая собой комплекс технических, программных, других средств и персонала, предназначенная для автоматизации различных процессов (в отличие от автоматической системы не может функционировать без участия человека)» [44, 250].

В то же время следует сказать, что существуют и другие понятия, относящиеся к обозначениям комплексов с включенными в них персональным компьютером: система ЭВМ, компьютерная сеть, сеть ЭВМ. Полагаем, в данном случае возникает необходимость установления сходств и (или) различий в данных терминах, с целью устранения неясностей и пробелов, возникающих и могущих возникнуть при получении информации с технических каналов связи при расследовании преступлений.

Под системой ЭВМ следует понимать комплекс, состоящий из нескольких взаимосвязанных компьютеров, составляющих единую систему. Система в ее классическом понимании — это объект, элементы которой находятся в упорядоченной зависимости. Отдельные авторы [56, 276; 71, 65] обоснованно утверждают, что любая компьютерная система характеризуется определенными параметрами:

1) тип системы;
2) общие технические возможности системы;
3) число входящих ПЭВМ (персональных ЭВМ);
4) место нахождения основных блоков системы, «ведущих» машин, основных накопителей информации и так далее.

Сети ЭВМ — это несколько ЭВМ, объединенных в единый комплекс посредством линии связи. Где, линия связи — физическая среда, по которой осуществляется передача данных между терминалами сети. В зависимости от ее характера, принципа построения, назначения и использования различают линии проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной и других видов связи [44, 248; 68, 178].

Необходимость создания таких комплексов возникает на крупных предприятиях (и между ПК физических лиц) для эффективного управления, а также решения различных задач и проведения операций. Различают локальные и глобальные сети. К локальной могут относиться сети в пределах одного или нескольких крупных предприятий или учреждений. Глобальные сети, типа «Интернет», в которых присутствует целая система обмена данных, позволяют осуществить доступ к данным ЭВМ на другом континенте. Сети ЭВМ являлись объектами исследования не только программистов, техников и других, но и криминалистов [72; 73; 74]. Проведенными исследованиями сетей ЭВМ определен ряд характеризующих их параметров:

1) общие технические возможности сети;
2) принадлежность сети к конкретной организации;
3) доступ к сети извне, их характеристика;
4) местоположение основных блоков сети, «ведущих» машин, локальные сети, входящие в ее состав.

Компьютерная сеть представляет собой ассоциацию, в которой ЭВМ взаимодействуют друг с другом, передают и получают информацию. Для связи между компьютерами, в информационных сетях применяются 4 вида каналов приема — передачи данных: прямые каналы; каналы, прокладываемые через телефонную и телетайпную сети; радиоканалы и космические спутники.

Все компьютерные сети можно разделить на два вида: территориальные и локальные.

Территориальной называют информационную сеть, компьютеры которой находятся на большом расстоянии друг от друга, обычно от 10-20 до десятков тысяч км. Она состоит из локальных сетей, а также многотерминальных систем и систем виртуального доступа.

Локальной является информационная сеть, компьютеры которой сосредоточены на небольшом расстоянии друг от друга, обычно в пределах до 10-20 км, а зачастую в одном здании [75, 16-17].

Рассмотрев основные виды и характеристики систем связи в сфере компьютерных технологий и исследуя вопрос соотношения норм уголовно-процессуального законодательства с иными нормативными актами по вопросам деятельности органов уголовного преследования по получению и использованию информации, полагаем необходимым обратиться к Закону РК «О связи», как основному нормативному акту, регламентирующему порядок и особенности использования средств связи и доступа к ним. Так в Законе Республики Казахстан «О связи» от 13 мая 1999 г. установлены правовые основы деятельности в сфере связи, определены полномочия органов государственной власти по урегулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи. Этим же законом к связи отнесены все сети и сооружения электрической и почтовой связи на территории нашей республики (за исключением внутрипроизводственных и технологических сетей связи).

Настоящим законом установлено, что средства связи вместе со средствами вычислительной техники составляют техническую базу обеспечения процесса сборки, обработки, накопления и распространения информации. А под понятием электрическая связь следует понимать всякую передачу или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам. Под сетями электросвязи Законом 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. Кроме определения основных понятий, используемых в сфере связи, в ст. 9 «Взаимодействие операторов связи с органами, осуществляющими оперативно-розыскную деятельность» указанного закона определено:

«ч. 1. Операторы связи, независимо от форм собственности и ведомственной принадлежности, действующие на территории Республики Казахстан, обязаны, в соответствии с законодательством Республики Казахстан, обеспечивать органам, осуществляющим оперативно-розыскную деятельность, организационные и технические возможности проведения оперативно-розыскных мероприятий на всех сетях связи, принимать меры по недопущению раскрытия форм и методов проведения указанных мероприятий.

ч. 2. В случае использования средств связи в преступных целях, наносящих ущерб интересам личности, общества и государства, государственные органы, в соответствии с законодательством Республики Казахстан, имеют право приостановления деятельности любых сетей и средств связи, независимо от ведомственной принадлежности и форм собственности» [76].

Таким образом, законодатель закрепляет полномочия органов полиции на вторжение в различные сети связи и проведение оперативно-розыскных меро-

приятий в них, а также воздействие на сети и средства связи (вплоть до отключения таковых), при наличии информации о готовящихся, совершаемых или совершенных преступлениях с использованием вычислительной техники и сетей электросвязи.

Исходя из приведенных выше трактовок, предлагается сформулировать понятия, отражающие содержание терминов, используемых в уголовном судопроизводстве при производстве процессуальных действий и составлении документов, связанных с получением информации при ее снятии с компьютерных систем. Думается, что данные понятия терминов необходимы для единообразного применения и оформления как процессуальной, так и оперативной документации.

Компьютер (персональный компьютер, ЭВМ) — 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. При описании компьютера необходимо

- отразить точное местонахождение компьютера и его периферийных устройств (принтера, модема, клавиатуры, монитора, джойстика, мыши, светового пера, микрофона, факс-модема, стримера, сканера, плоттера и других);
- определить и указать тип, модель и иные характеристики устройств, входящих в состав ЭВМ; назначение каждого устройства, название (обычно указывается на лицевой стороне), номер модели и серийные номера, инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия; комплектацию (наличие и тип дисководов, сетевых карт, разъемов и так далее), наличие соединения с локальной вычислительной сетью и (или) сетями телекоммуникации, состояние устройств (целое или со следами вскрытия); прочую информацию с фабричных ярлыков;
- установить наличие внутри компьютера нештатной аппаратуры, а также внутренних накопителей и устройств для работы с другими машинными носителями (дискеты, компакт-диски, магнитооптические диски и другие);
- точно описать порядок соединения между собой указанных устройств, промаркировав (при необходимости) соединительные кабели и порты их подключения. При наличии отключенных внешних периферийных устройств (модема, сканера, принтера и других) указать на возможность их подключения. Проверить их работу с исследуемым компьютером (при возникновении такой необходимости) можно в ходе следственного эксперимента.

Компьютерная система (вычислительная система, локальная система, автоматизированная система, система ЭВМ) — это любая система, в состав кото-

рой входит компьютер, предназначенный для управления этой системой либо для принятия решений, а также включающая в себя аппаратное (совокупность технических устройств и приборов, используемых в работе с компьютером) и программное (совокупное название программных и информационных ресурсов, используемых в работе с компьютером) обеспечение и персонал, действующих совместно. При описании исследуемой компьютерной системы необходимо указать: тип системы, общие технические возможности системы, число входящих ПЭВМ, место нахождения основных блоков системы, «ведущих» машин, основных накопителей информации и так далее.

Компьютерная сеть (сеть ЭВМ) — единый комплекс, в котором ЭВМ взаимодействуют друг с другом, передают и получают информацию посредством каналов связи. В составе компьютерной сети различают локальные и глобальные сети.

Локальная компьютерная сеть — компьютеры данной сети сосредоточены в пределах одного или нескольких предприятий или учреждений на небольшом расстоянии друг от друга (обычно до 10-20 км), а зачастую в одном здании.

Глобальная компьютерная сеть — компьютеры данной сети находятся на большом расстоянии друг от друга (от 10-20 до десятков тысяч км), имеющая систему обмена данных, позволяющую осуществить доступ к данным из ЭВМ на другом континенте. Она состоит из локальных сетей, а также многотерминальных систем, систем виртуального доступа и других.

Сеть ЭВМ характеризуется рядом параметров:

1) общие технические возможности сети;
2) принадлежность сети к конкретной организации;
3) доступ к сети извне, ее характеристика;
4) местоположение основных блоков сети, «ведущих» машин, локальные сети, входящие в ее состав.

Канал связи — часть сети, связывающая между собой каждую пару ее оконечных терминалов и состоящая из технических средств передачи и приема данных, включая линию связи, а также средств программного обеспечения и протоколов. В зависимости от характера, принципа построения, назначения и использования различают каналы проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной, аналоговой, цифровой, дуплексной (двухсторонней) связи и так далее.

Линия связи — физическая среда, по которой осуществляется передача данных между терминалами сети. В зависимости от ее характера, принципа построения, назначения и использования различают линии проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной и других видов связи.

Электрическая связь — всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической, и другим электромагнитным системам.

Сети электросвязи — 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.

Компьютерные системы и объединяющие их технические каналы связи, как объекты процессуальных действий, являются носителями огромного объема информации, могущей иметь значение для расследуемых дел — сведения о преступных группировках, готовящихся и совершенных ими преступлениях, способах их сообщения, передачи информации, формах расчета и многое другое. Знание и использование возможностей компьютерных достижений позволит правоохранительным органам более качественно противостоять преступной деятельности.

2 ПЕРЕХВАТ СООБЩЕНИЙ КАК САМОСТОЯТЕЛЬНОЕ СЛЕДСТВЕННОЕ ДЕЙСТВИЕ

2.1 Перехват сообщений как специальный процессуальный способ получения информации

Стремительно развивающиеся системы связи и телекоммуникации общего пользования, их повышенная мобильность и конфиденциальность активно используются лицами, совершающих преступления. В связи с чем, для сотрудников полиции становятся актуальными задачи эффективного контроля переговоров и сообщений лиц, имеющих отношение к подготовке и совершению преступлений. Однако такой контроль наряду с положительной имеет и отрицательную сторону. Он заведомо влечет ограничение конституционных прав граждан. Любое же ограничение прав и свобод человека и гражданина в соответствии со ст. 18 Конституции РК допустимо только в случаях и в порядке, прямо установленных законом [77]. Такими Законами являются: Закон РК «Об Оперативно-розыскной деятельности» от 12 августа 1995 г., с изменениями и дополнениями от 10 ноября 2001 г., [78] и Уголовно-процессуальный кодекс. Несмотря на то, что данные законы допускают проведение мероприятий по прослушиванию телефонных переговоров и сообщений, правовой механизм использования результатов недостаточно отрегулирован. Среди профессионалов долгое время не прекращаются споры о возможности использования в качестве доказательств в уголовном процессе результатов прослушивания переговоров и перехвата сообщений. Кроме того, порядок хранения фонограмм, условия их прослушивания, тиражирования и уничтожения определялся закрытыми нормативными правовыми актами.

Существенным шагом на пути правового разрешения указанных вопросов стало принятие Уголовно-процессуального кодекса Республики Казахстан, введенного в действие в 1998 г., содержащего ст. 236 «Перехват сообщений». Однако отметим, что законодатель не раскрыл содержания понятия «перехват сообщений», позволяющее определить границы проводимого действия, в связи с чем, оно может рассматриваться достаточно широко и неоднозначно.

По мнению Б. М. Нургалиева и М. А. Арыстанбекова «перехват сообщений, передаваемых по техническим каналам связи, заключается в том, что информация, идущая по контролируемым каналам, может быть в пути следования задержана, приостановлена, отделена от оригинала в виде копии, зафиксирована на соответствующем носителе» [79, 174]. Соглашаясь в целом с предложенным определением, тем не менее, следует указать, что оно требует более детального рассмотрения и разъяснения терминов операций, проводимых над информацией. Обратившись к словарю русского языка под редакцией С. И. Ожегова, мы найдем следующее толкование «перехвата»: «1) схватить на пути следования, 2) схватить в каком-нибудь месте».

Данное толкование не дает полного содержания термина в интересующем нас уголовно-процессуальном аспекте. В связи с этим, исследуя сходные по смыслу термины — «снятие» и «изъятие», мы получим следующую информацию: «снять — 1) достать, взять, убрать, отделить находящееся сверху, 2) лишить чего-нибудь, освободить от чего-нибудь, 3) изготовить (сделав копию оригинала)» [4, 650].

Изъятие (в уголовном процессе) — отчуждение (или получение) предметов или документов, происходящее при производстве следственных действий [80, 12].

Как видно из приведенных выше толкований каждое определение, если оно применяется в сфере своего действия, верно отображает какую-то одну сторону или особенность действия. В связи с этим возникает необходимость универсализации частного определения «перехвата» при решении задач уголовного судопроизводства. Обобщив указанные толкования можно прийти к выводу, что перехват — это действие, которое позволяет схватить на пути следования какое-либо сообщение, лишить его (чего-нибудь) части информации, сделать копию оригинала, (убрать) уничтожить сообщение, (отчуждение) изъять его или направить адресату.

Однако данная формулировка не раскрывает в полной мере процессуальное содержание перехвата сообщений, а также порядок и особенности производства операций над передаваемыми сообщениями, компьютерной информацией. Потому, полагаем вполне обоснованным, обратиться к научным исследованиям и специальной литературе в области уголовно-процессуального права, информатики и информации, определяющим порядок работы с компьютерной информацией. Так, профессор Н. А. Селиванов предлагает следующие понятия терминов по обработке информации: «уничтожение информации — означает прекращение существования важных сведений на магнитных носителях и в оперативной памяти ЭВМ, приведение в такое состояние, когда они не могут быть восстановлены и использованы по назначению; блокирование информации — искусственное создание таких условий эксплуатации ЭВМ, когда становится невозможным получение или использование компьютерной информации по назначению при ее полной сохранности (невредимости); модификация информации — любые изменения не направленные на обеспечение интересов собственника или иного владельца информационных ресурсов» [81].

Заслуживает внимания и трактовка отдельных понятий терминов, приводимых В. Б. Крыловым в учебном пособии по компьютерным преступлениям, где под блокированием компьютерной информации понимается воздействие на компьютерную информацию, делающее ее недоступной для владельца, при сохранности такой информации; модификация компьютерной информации — преобразование ее логической и физической организации; копирование компьютерной информации — создание дубликата файла на машинном носителе [65, 76]. Говоря о блокировании информации, отметим, что в ч. 2 ст. 9 Закона РК «О связи» от 13 мая 1999 г. определено: «В случае использования средств связи в преступных целях, наносящих ущерб интересам личности, общества и государ-

ства, государственные органы, в соответствии с законодательством Республики Казахстан, имеют право приостановления деятельности любых сетей и средств связи, независимо от ведомственной принадлежности и форм собственности» [80].

Ю. Гульбин, исследуя вопросы терминологии операций над информацией, под уничтожением информации понимает лишение сведений, данных и прочей соответствующей материальной формы; а под блокированием — лишение возможности правомерного пользователя реализовывать информацию ЭВМ по назначению [82, 32].

Проанализировав различные мнения и понятия терминов, связанные с обработкой информации, предлагается универсальная, но не претендующая на роль исключительной интерпретация основных понятий терминов, входящих в содержание перехвата сообщений и компьютерной информации, передаваемой по техническим каналам связи. Предлагается следующая трактовка понятий.

Копирование информации — снятие копии и (или) создание дубликата файла(ов) на машинном носителе с оригинальной информации с сохранением ее неповрежденности и возможности использования по назначению. Данная операция (копирование) является наиболее распространенной в работе с компьютерной информацией, но по-разному находит свое отражение в процессуальных документах. Например, при осмотре сведений в компьютере гражданина О., часть информации, имеющая отношение к делу, была скопирована на магнитный носитель. При этом в протоколе осмотра была сделана следующая запись: «… при исследовании информации, содержащейся в компьютере в папке “7567564”, имеющей путь — С/мои документы/разные дела/свое/, обнаружен файл “2000” — являющийся рисунком, содержащим точную копию купюры достоинством 2000 тенге. Данный файл, в присутствии понятых, скопирован на чистую дискету, упакован и опечатан печатью» [69]. В деле № 1252251203, при осуществлении обыска в квартире подозреваемой К., в протоколе обыска указано: «в домашнем компьютере К. обнаружен текстовый файл, содержащий список фамилий, напротив которых стояла сумма полученных денег. Также имеется фамилия П., который является потерпевшим по данному делу. Данный файл скопирован на дискету 3.5 Мб, черного цвета, путем выполнения следующих команд — выделить файл, копировать, отправить на диск 3,5 (А)» [83].

Блокирование информации — искусственное создание таких условий эксплуатации ЭВМ или воздействие на компьютерную информацию, когда становится недоступным, невозможным получение или использование информации по назначению при ее полной сохранности (невредимости). Блокирование может быть осуществлено путем запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, или выключения реакции какого-либо устройства ЭВМ. Блокирование сообщения производится на срок, установленный следователем в постановлении о назначении перехвата сообщений. Срок блокирования определяется в зависимости от следственно-оперативной необходимости и не должен превышать сроков расследования. Одним из примеров блокирования информации является ситуация,

когда следователем был изъят компьютер, в котором предположительно могли храниться сведения, представляющие интерес для следствия. Так как следователь не имел достаточных навыков для качественного исследования компьютерной информации, то он в целях недопущения доступа посторонних лиц к базе данных компьютера, до момента возможности привлечения специалиста к осмотру ЭВМ, поставил пароль на запуск операционной системы, блокировав, таким образом, информацию от нежелательного доступа.

Уничтожение информации — прекращение существования информации полностью либо в ее части, на магнитных носителях и в оперативной памяти ЭВМ, приведение в такое состояние, когда она не может быть восстановлена и использована по назначению. Уничтожение информации производится на основе решения следователя, после просмотра перехваченных сообщений. Информация может быть уничтожена в случаях, когда перехваченные сообщения не представляют интереса для следствия или не могут быть использованы в доказывании (например, файлы повреждены и не подлежат восстановлению, пароль на файл не может быть взломан, либо на его взлом потребуется времени, больше срока расследования и другое). Кроме того, уничтожение может быть произведено в тех случаях, когда обнаружена информация, носящая секретный, совершенно секретный характер, сведения, составляющие государственную или иные виды тайн и (или) дальнейшее сохранение у лица полученной информации или ее направление адресату недопустимо. Так, при расследовании дела по факту фальшивомонетничества с использованием компьютерной техники, у подозреваемого В. в домашнем компьютере был обнаружен файл, содержащий сканированную версию банкноты достоинством 100 долларов США. После копирования данного файла на дискету, файл из памяти компьютера был уничтожен. В протоколе осмотра данная операция была отражена следующим образом: «файл “деньги”, имеющий размер 89 Кб, удален из памяти путем выполнения следующих команд — “выделить файл, удалить, ОК” — “открыть корзину, выделить файл “деньги”, удалить безвозвратно, ОК”» [69].

При производстве перехвата сообщений как оперативно-розыскного мероприятия может применяться и такая операция как «модификация информации», под которой следует понимать — изменение первоначальной информации полностью либо в ее части с последующим направлением модифицированного сообщения адресату. Данная операция должна производится в соответствии с требованиями Закона об оперативно-розыскной деятельности и специальных нормативных актах, регулирующих данное положение.

Кроме содержательной стороны обозначенных выше понятий, необходимо акцентировать внимание на том, что проведение соответствующих действий требует участия специально подготовленных сотрудников (к сожалению таких единицы), а также оснащения правоохранительных органов соответствующей аппаратурой и программным обеспечением. Для улучшения качества производства перехвата сообщений, возможно приглашение специалистов в области информатики или поручения производства перехвата сообщений организациям, предоставляющим услуги в сфере информационных технологий в порядке,

определяемом уголовно-процессуальным законодательством. Данный вывод подтверждается тем, что в 80 % исследованных дел, расследование которых было связано с использованием, исследованием компьютерной техники и информации, следователями для производства следственных действий приглашались специалисты в области компьютерных технологий.

Принятие Уголовно-процессуального кодекса Республики Казахстан заставило по-новому пересмотреть устоявшиеся взгляды на некоторые институты уголовно-процессуального права, поставило перед фактом появления новых правовых институтов, позволяющих расширить доказательственную базу путем использования в доказывании информации, полученной с технических каналов связи, компьютерных систем, в том числе и при производстве оперативно-розыскных мероприятий. Рассматривая сущность перехвата сообщений, невольно возникает вопрос: «С чем связано появление нового следственного действия и чем оно отличается от уже действующих?». Проводя анализ, мы пришли к выводу, что перехват сообщений можно сравнивать, выявляя особенности и специфику, с такими следственными действиями как прослушивание телефонных переговоров и обыск. Схожие положения норм и отдельные аспекты, подлежащие исследованию и проработке, видны из приведенного ниже анализа (см. таблицу № 1).

Таблица 1 — Соотношение перехвата сообщений с обыском и прослушиванием телефонных переговоров

Обыск (ст. ст. 230, 232, 233 УПК РК)	**Перехват сообщений (ст. 236 УПК РК)**	**Прослушивание телефонных переговоров (ст. 237 УПК РК)**
1	**2**	**3**
Цель — обнаружение и изъятие предметов или документов, имеющих значение для дела. **Объект исследования** — помещения, земельные участки, вещи, предметы, и другое. **Метод —** допустимо принудительное проникновение, использование взлома преград. **Предмет исследования** — любые объекты, имеющие значение для дела.	**Цель —** обнаружение информации, передаваемой по техническим, компьютерным каналам связи. **Объект исследования** — компьютерная система, компьютерная сеть, технические каналы связи. **Метод —** использование спецсредств, взлом не предусмотрен, но может быть допустим, при наличии пароля на сообщение. **Предмет исследования** — информация, относящаяся к расследуемому делу.	**Цель —** обнаружение сведений, имеющих значение для дела. **Объект исследования** — телефонные лини связи, переговорные устройства. **Метод —** использование прослушивающих и записывающих устройств. **Предмет исследования** — информация, представляющая интерес для расследования.

Продолжение таблицы 1

1	2	3
Срок действия — разовый. **Санкция прокурора** — обязательна, но есть исключительные случаи. **Участие специалиста** — необходимость определяется следователем.	**Срок действия** — не определен, но может быть разовым или продолжительным. **Санкция прокурора** — обязательна. **Участие специалиста** — необходимо.	**Срок действия** — продолжительный (до 6 месяцев). **Санкция прокурора** — обязательна, но есть исключительные случаи. **Участие специалиста** — необходимо.

Из приведенной таблицы видно, что перехват сообщений включает в себя как положения обыска, так и прослушивание переговоров. В связи с отсутствием нормативной документации по разъяснению сущности перехвата сообщений (который может являться как разновидностью обыска, так и электронной формой прослушивания) позволим себе обратиться к правовой истории регламентации перехвата сообщений на основе опыта зарубежных стран, в частности, Соединенных Штатов Америки.

До периода бурного развития технических средств электронного наблюдения и подслушивания судебная практика США исходила из того, что запрет необоснованных обысков, как гарантия соблюдения прав граждан на частную жизнь, распространяется только на материальные объекты (дом, машину, контору, личные вещи и бумаги). Нарушение этого запрета приводило к исключению из рассмотрения судом незаконно изъятых вещественных доказательств, то есть суды отождествляли право собственности индивида и сферу его частной жизни.

Появление электронных подслушивающих и звукозаписывающих устройств предоставило возможность правоохранительным органам «изымать» мысли, желания, намерения граждан, воплощенные в слова, то есть все то, что формирует частную жизнь гражданина, и осуществлялось, причем совершенно безнаказанно, так как не было оснований для применения правила об исключении доказательств, полученных незаконным путем. Верховный суд США был вынужден признать, что в условиях постоянно развивающейся технологии подслушивания защита частной жизни граждан требует большего, чем простой запрет необоснованного физического нарушения владения и изъятия материальных предметов. Таким образом, единственным подходом к сдерживанию негативных проявлений научно-технических достижений явилась выработка стандартов и создание процедур, гарантирующих право на частную жизнь.

Противники подслушивания утверждали, что оно неконституционно по своей природе, так как представляет собой, в сущности, «общий обыск», поскольку при подслушивании практически невозможно предсказать, какая часть

разговора или весь разговор может стать доказательством обвинения. Они обосновывали это тем, что, даже если принять подслушивание за «обыск», то в ордере на такой «обыск» просто невозможно включить «подробное описание» предмета, подлежащего изъятию, поскольку подслушивание ведется «вслепую», пока не будет зафиксирован интересующий разговор. Как пишет Р. Кларк, бывший генеральный атторней США, подслушивание «улавливает все, что происходит в мире звуков, не будучи, однако, в состоянии отличить рыбу от мяса ...». Именно поэтому противники подслушивания считают его грозным орудием вторжения в частную жизнь граждан.

Сторонники же подслушивания указывают на его эффективность в деле борьбы с преступностью вообще, а в особенности с такой ее разновидностью, как организованная преступность.

При оценке правовой регламентации прослушивания необходимо иметь в виду не столько строгость этой регламентации, сколько сам факт узаконения прослушивания и признания его вполне конституционным методом сбора доказательств. «Общий обыск», который авторы «Билля о правах» пытались исключить из правоприменительной деятельности, дабы оградить человека от произвола властей, институционализировался в современной конституционной практике США посредством достижений электронной техники.

Таким образом, научно-технический прогресс XX в. положил начало возникновению и развитию новой специфической формы обыска — электронному прослушиванию и наблюдению.

Особенностью уголовного процесса США того времени являлось то, что в нем электронное прослушивание и наблюдение рассматривалось по своим юридическим последствиям к обыску, а поэтому должно было осуществляться «… на основании ордера, т. е. под контролем судебной власти». Отметим, что применительно к законодательству Республики Казахстан, и обыск, и прослушивание телефонных переговоров производится на основании санкции прокурора, то есть под контролем должностного лица, осуществляющего в пределах своей компетенции надзор за законностью оперативно-розыскной деятельности, дознания, следствия и судебных решений, а также уголовное преследование на всех стадиях уголовного процесса. Полномочия прокурора при досудебном производстве и рассмотрении дела судом определяются соответственно ст. ст. 190, 192 (ч. 6 и ч. 7), 197, 289, 317, 396 (ч. 3), 458, 460 УПК РК.

В связи с тем, что любое прослушивание было приравнено по своим юридическим последствиям к обыску и изъятию оно, без надлежащего образа оформленного ордера, становилось незаконным. Результаты же незаконного прослушивания, как и результаты незаконного обыска, не могли впредь рассматриваться в суде в качестве доказательств.

Но следует заметить, что есть разница между обычным обыском и любым электронным прослушиванием. Установлено, что обыск без соответствующего нового ордера недопустим. В противоположность, этому прослушивание предполагает относительную продолжительность тайного вторжения в частную

жизнь с целью поиска доказательного материала, который может появиться лишь предположительно.

С другой стороны, исполнение ордера на обыск завершается изъятием заранее определенных, по крайней мере, по родовому признаку, объектов. По общему правилу никакие иные объекты (за исключением точно обозначенных в законе) изыматься не могут. Во время же прослушивания невозможно точно установить, что из перехваченной информации будет иметь доказательственное значение.

Наконец, невозможно определить при прослушивании, что здесь является обыском, а что изъятием. Само прослушивание расценивается как длящийся обыск. Но Верховный суд США в решениях по делам указанной специфики не установил и не разъяснил, когда же происходит «изъятие» доказательств: в момент самого прослушивания, его записи или непосредственного использования в суде. Следовательно, привязка электронного прослушивания к обыску и изъятию доказательств носит несколько условный характер. В силу сложившихся традиций Верховный суд США «проигрывал» новые процессуальные правоотношения через призму стабильной и неизменной Конституции, что приводило к ряду противоречий, которые обычно преодолеваются судебной практикой. Перехваты телеграфных сообщений стали настолько распространены, что, например, в Калифорнии в 1862 г. был принят специальный закон, запрещающий такую практику. В 1895 г. такая практика была запрещена в двух штатах, а в 1905 г. в Калифорнии запрещение телеграфных перехватов было распространено и на телефонные переговоры [84].

На основе происходящих попыток законодателя выработать нормы, регулирующие электронный перехват, Верховный суд США столкнулся с необходимостью дать толкование поправки IV применительно к подслушиванию телефонных разговоров. Впервые это было в 1928 г. Суд постановил, что поправка IV, запрещающая необоснованный обыск, под которым следует понимать «физическое вторжение в чужое владение изъятие материальных предметов», не распространяется на подслушивание телефонных разговоров, так как в этом случае не происходит ни нарушения прав собственности, ни изъятия предметов. Таким образом, был создан прецедент, узаконивший беспрепятственное вторжение правоприменительных органов в сферу частной жизни граждан с целью получения инкриминирующих доказательств, при помощи любых технических средств, установка которых не требовала нарушения права собственности.

Но адвокаты и юристы в целях признания результатов подслушивания телефонных разговоров недопустимыми доказательствами длительное время использовали в суде положения закона о средствах связи (1934 г.), в котором содержался запрет перехвата и разглашение любых сообщений, переданных по радио или по проводам. Исходя из формулировки закона, противоправным считается не столько подслушивание телефонных разговоров, сколько разглашение их содержания. Поэтому в деле Нардона (1939 г.) основанием для отклонения результатов подслушивания явился не сам факт незаконного вторжения правоприменительных органов в сферу личной жизни гражданина, а то, что показа-

ния полицейского на суде о содержании подслушанного им разговора представляли собой его «разглашение», по смыслу Закона о средствах связи. Но в то же время, звукозапись разговора, подслушивание которого осуществлялось с согласия одной из сторон, участвовавших в беседе, считалась допустимым доказательством, так как было определено, что в этом случае нет «перехвата». Таким образом, закон о средствах связи отнюдь не стоял на страже интересов соблюдения тайны частной жизни граждан.

Нельзя правда считать, что юристы США единодушны в решении вопроса о допустимости полученных таким способом доказательств. Так, судья Дуглас, член Верховного суда США, отметил: «Условие о соблюдении требований поправки IV к Конституции не должно быть связано с видом применяемого электронного оборудования. Единственное, что заслуживает внимание — это право на тайну частной жизни, которое было нарушено». Этот высказывание отражает созревшую в середине 60-х годов в США необходимость пересмотреть традиционное толкование поправки IV [85].

Так созревала новая трактовка поправки IV к Конституции, при этом происходила переоценка конституционности тех или иных действий полиции. В этом плане своеобразной вехой в США явилась выработка понятия частной жизни граждан. В соответствии с которым в толковании поправки IV было указано, что она направлена «на охрану личности, а не места или помещения». По мнению Верховного суда США, «все, что индивид сознательно обнародует, предает гласности — не является объектом конституционной защиты, но все то, что он намерен скрыть от посторонних глаз или ушей, подлежит охране Конституцией. Человек, закрывающий за собой дверь в телефонную будку, имеет все основания рассчитывать, что содержимое его разговора останется в тайне» [85]. Тем самым, Верховный суд установил новый прецедент, в соответствии с которым, основанием для признания доказательств недопустимыми считается не только незаконное физическое вторжение в жилище и вообще конституционно охраняемую область материальных объектов, но и любое необоснованное посягательство на частную жизнь граждан, каковым являются, в частности, подслушивание телефонных и других разговоров с помощью технических устройств. Исходя из анализа новой трактовки следует, что обыск — это нарушение обоснованно ожидаемой неприкосновенности частной жизни.

Таким образом, судебная практика и законодательство США, установив практически аналогичные условия правомерности проведения обычного обыска и электронного прослушивания, по существу снизили уровень требований к допустимости доказательств, полученных путем электронной слежки.

Действующая традиционная схема правового регулирования, рассмотренная выше, была изменена 19 июня 1968 г., когда Конгресс США принял объединенный Закон «О контроле над преступностью и обеспечением безопасности на улицах». Третий раздел этого закона, озаглавленный «Подслушивание телефонных переговоров и электронное прослушивание», включил в 18 раздел Свода законов США новую главу 1-119, призванную урегулировать и унифицировать полицейскую практику в этом вопросе. В новом законе была пред-

принята попытка сбалансировать потребности правоприменяющих органов в борьбе с преступностью и защиту граждан от необоснованного вторжения государства в их частную жизнь. Кроме того, был введен ряд ограничений, не предусмотренный ранее в решениях Верховного суда. Прежде всего, был четко ограничен круг преступлений (правда, весьма широкий), при расследовании которых могло применяться прослушивание (§ 2516 [1], [2]). Закон запретил любые прослушивания с помощью любых устройств без соответствующего судебного ордера. При этом правила подслушивания различались в отношении устных переговоров (oral communication) и переговоров с помощью проводных средств связи (wire communication). Первые, на основании ордера, должны подслушиваться лишь в тех местах, которые конституционно охраняются от государственного вторжения (квартира, место работы, номер в отеле и так далее). Для подслушивания в иных местах, например, в тюрьме, ордер не требовался (§ 2510 [2]). Во втором случае прослушивание без ордера вообще запрещалось (§ 2510 [11]) [86].

Конечно, электронное наблюдение как специфическая форма обыска — объективный факт социальной действительности США. Но введение «стихии» электронного наблюдения в русло закона имеет определенное положительное значение. Закон стал правовой базой, опираясь на которую, обвиняемый может оспаривать законность предпринятых против него действий полиции и ходатайствовать об исключении полученных при этом доказательств.

На основании изложенного следует констатировать, что проблема правомерности и целесообразности использования правоохранительными органами средств электронного наблюдения является весьма актуальной уже на протяжении ряда десятилетий, и включение такой нормы как «Перехват сообщений» в сферу уголовного судопроизводства Республики Казахстан является первым шагом казахстанского законодателя в решении данной проблемы.

Полагаем, что отнесение перехвата сообщений к разновидности электронного прослушивания переговоров непозволительно. На основе развития функционирования института электронного перехвата США видно, что смешение различных норм или использование порядка осуществления одного следственного действия для другого, в чем-то даже и схожего, недопустимо. Это связано с тем, что положения одной нормы могут (и будут) не соответствовать или противоречить специфике производства другой, что, в конечном счете, повлияет не только на решение вопроса о допустимости доказательств, но и повлечет за собой нарушение законов государства, конституционных прав личности и неправомерного решения судьбы лиц, попавших в сферу уголовного судопроизводства. В подтверждение этого еще раз обратим внимание, что законодатель США (после многих неудачных попыток объединения следственных действий) принял специализированный нормативный правовой акт, регулирующий специфику применения электронных форм контроля.

Таким образом, перехват сообщений передаваемых по техническим и компьютерным каналам связи является самостоятельным следственным действием и под ним следует понимать действия органа уголовного преследования, а так-

же физических или юридических лиц по поручению органа уголовного преследования, направленные на копирование, блокирование, изъятие и уничтожение, передаваемой информации, с целью получения доказательств по делу.

Перехват сообщений является самостоятельным следственным действием, поскольку имеет отличие от других следственных действий по своей цели — обнаружение информации, передаваемой по техническим, компьютерным каналам связи; объекту — компьютерная система, компьютерная сеть, технические каналы связи; методу — использование специальных средств при получении, исследовании информации, осуществлению взлома при наличии пароля на сообщение; задачам — копирование, блокирование, изъятие, уничтожение информации и порядку его осуществления.

Так как перехват сообщений в сфере уголовного судопроизводства является новым следственным действием, то порядок его функционирования требует более детальной разработки и законодательного закрепления в нормативно-правовой базе Республики Казахстан. В связи с чем, полагаем необходимым определить процессуальный порядок производства перехвата сообщений и более детально остановиться на каждом из аспектов его реализации.

Считаем, что перехват сообщений, как следственное действие, направленное на получение информации с технических каналов связи и снятие информации с компьютерных систем должно иметь следующий порядок:

- определение цели и оснований для производства перехвата сообщений;
- определение объекта и системы, в которой планируется производство перехвата;
- определение участников проводимого действия;
- определение органа, осуществляющего перехват;
- определение срока и порядка передачи перехваченной информации;
- вынесение постановления;
- санкционирование постановления прокурором;
- получение перехваченной информации от исполняющего органа;
- осмотр полученной информации и принятие решения о ее дальнейшей судьбе.

На основании вышеизложенного также предлагается дополнить ст. 236 УПК РК частью, в следующей редакции: «Полученная при перехвате сообщений информация копируется на машинный носитель, после чего по решению органа уголовного преследования может быть направлена адресату, блокирована, изъята или уничтожена. Операции, проводимые над информацией, отражаются в протоколе осмотра предметов и документов, согласно требованиям, установленными статьями 221, 222, 223, 227 УПК РК».

2.2 Цели, основания и объект перехвата сообщений

Говоря сегодня об основных тенденциях информационного обеспечения деятельности правоохранительных органов, необходимо учитывать не только

возможности, которые представляют современные компьютерные технологии и средства специальной техники, но и негативные процессы в обществе, которые связаны с обострением развития организованной преступности, коррупции, уголовного терроризма, теневой экономики.

Одно из существенных обстоятельств, которое необходимо принимать во внимание в первую очередь состоит в том, что внедрение информационных технологий практически во все области жизни включает и последовательную «информатизацию» самых разнообразных сфер преступной деятельности. Сегодня становится очевидным, что общество сталкивается с проблемой применения «высоких технологий» как для подготовки и осуществления преступлений, так и для ухода от ответственности, а также и для противодействия правоохранительным органам [15, 311].

Сотрудниками Комитета национальной безопасности РК отмечено, что «существенное повышение эффективности борьбы с современной преступностью может быть достигнуто на пути широкого использования возможностей современных информационных технологий и специальной техники. Это требует, в свою очередь, формирования и развития новых направлений информационно-технического обеспечения оперативно-розыскной и следственной деятельности» [70, 386].

Рассматривая опыт зарубежных стран по формированию законодательства в сфере использования компьютерных технологий при расследовании преступлений, следует заметить, что наличие правовой нормы не всегда позволяет осуществить регламентируемое ею положение на практике. Так, на примере США (как одного из государств, которые в числе первых стали применять электронное прослушивание), мы можем проследить стадии формирования норм, регулирующих порядок перехвата сообщений, и на основе этого выработать механизм перехвата сообщений с технических каналов связи применительно к законодательству Республики Казахстан.

В 1968 г. Конгресс США принял объединенный Закон «О контроле над преступностью и обеспечением безопасности на улицах». В новом законе была предпринята попытка сбалансировать потребности правоприменяющих органов в борьбе с преступностью и защиту граждан от необоснованного вторжения государства в их частную жизнь. В данном Законе был четко ограничен круг преступлений (правда, весьма широкий), при расследовании которых могло применяться прослушивание. Также Закон запретил любые прослушивания с помощью любых устройств без соответствующего судебного ордера, сделав однако оговорку, что «допускается прослушивание без ордера, если хотя бы один из участников разговора добровольно разрешает сделать это» [86].

В 1986 г. Конгресс США, учитывая появление новых технологий в области связи, провел реформу законодательства о прослушивании. Нововведения затронули электронную почту, компьютерные сети, видеотелефоны, спутниковую телесвязь, некоторые виды радиосвязи. Окончательно легализовано электронное подслушивание с разрешения и под контролем судебных органов для расследования многих тяжких преступлений — взяточничества, похищения

людей, незаконной торговли наркотиками, убийств, грабежей, игорного бизнеса, предусмотрена возможность проведения электронного наблюдения без ордера при наличии «чрезвычайных обстоятельств», в силу которых органы расследования не имеют времени на получение ордера в надлежащем порядке.

Таким образом, проблема получения и использования в доказывании компьютерной криминальной информации представляется чрезвычайно актуальной. Широкое использование для обработки информации локальных и глобальных вычислительных сетей делает чрезвычайно перспективным разработку соответствующих методов получения информации, позволяющих расширить доказательственную базу путем использования в доказывании информации, полученной с технических каналов связи, компьютерных систем, в том числе и при производстве оперативно-розыскных мероприятий.

Необходимость исследования и разработки правил производства перехвата сообщений именно в сфере уголовно-процессуального законодательства подтверждается и рекомендациями отдела Европейского парламента по оценке научно-технологических разработок, согласно которым: «Использование всех технологий и осуществление мероприятий по перехвату сообщений в условиях демократического общества должно находиться под соответствующим контролем; необходимо разработать процессуальный кодекс с тем, чтобы в случае нарушения соответствующих правовых норм при проведении вышеупомянутых мероприятий можно будет внести необходимые коррективы. Необходимо также четко определить критерии в отношении способов хранения, обработки и использования полученной таким образом информации. Данный критерий и процессуальный кодекс, о котором говорилось выше, должны быть преданы гласности» [87].

Рассматривая процесс использования информации в сфере уголовно-процессуального законодательства, следует отметить, что основным способом доказывания преступных деяний и информации криминального характера является производство следственных действий, которые представляют собой «приспособленные к получению и передаче определенного вида информации комплексы познавательных и удостоверительных приемов, операций по обнаружению, собиранию и проверке доказательств, предусмотренные процессуальным законом и осуществляемые следователем, лицом, производящим дознание или прокурором» [60, 383]. Каждое следственное действие производится при наличии определенной цели и достаточных оснований для их проведения. Этого нельзя сказать о ряде следственных действий, хотя их цели достаточно полно определены во многих научных исследованиях, авторы которых неоднократно предлагали закрепить их в законе. Например, в ст. 235 «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка» и ст. 237 «Прослушивание и запись переговоров» отсутствуют цели данных действий, а указаны только основания, под которыми следует понимать достаточные данные о возможности достижения цели следственного действия.

В то же время в Уголовно-процессуальном кодексе точно указаны цели отдельных следственных действий (например, осмотр — ст. 221 УПК РК, обыск

— ст. ст. 230, 233 УПК РК). Анализируя цели ряда следственных действий (например, следственный эксперимент, очная ставка, предъявление для опознания, проверке показаний на месте) можно сказать, что они имеют одну общую цель — получение информации, проверку и уточнение данных, имеющих значение для дела. Между тем определенные следственные действия имеют специфические цели. Например, цель следственного эксперимента (ст. 239 УПК РК) — установление возможности существования какого-либо факта, совершения определенных действий, наступления определенных событий в конкретной обстановке. Специфической целью предъявления для опознания (ст. 228 УПК РК) является установление тождества или различия предъявляемого объекта с объектом, сохранившимся в памяти опознающего. Говоря о цели проверки и уточнения показаний на месте законодатель выделяет несколько задач — выявление достоверности показаний путем их сопоставления с обстановкой происшедшего события; уточнение маршрута и места, где совершались проверяемые действия и установление новых фактических данных и так далее.

Исходя из изложенного можно сделать вывод, что точное определение цели есть необходимый элемент полной регламентации оснований и порядка проведения следственного действия.

Таким образом, при проведении следственного действия, следователь (дознаватель) на основании положений Уголовно-процессуального кодекса, и, исходя из установленных целей, закрепляет получаемую информацию и использует ее для раскрытия преступлений. Так, при выемке почтово-телеграфной корреспонденции следователь непосредственно воспринимает содержание документа, после чего решает — изъять его или нет. Ничего этого нет при «перехвате сообщений». В ст. 236 УПК РК не сказано, как данное действие следователем осуществляется, хотя применительно к другим следственным действиям процедура получения и закрепления информации регламентировала вполне конкретно. И это неудивительно, так как фактическое получение информации осуществляет не следователь, а «орган, осуществляющий оперативно-розыскную деятельность». Следователю же остается принять и просмотреть компьютерную информацию, представленную ему сотрудниками органа дознания. Закрепляя данную норму, законодатель не указал цели и фактические основания производства перехвата сообщений, ограничившись лишь формулировкой: «перехват сообщений и снятие с компьютерных систем информации … производится на основании постановления следователя, санкционированного прокурором». Хотя следует отметить, что в большинстве случае именно фактические основания дают возможность производства следственного действия (естественно при процессуальном их оформлении — на основании постановления следователя).

Требование закона о допустимости перехвата сообщений «на основании постановления следователя» означает, что такой вывод должен вытекать из установленных по делу обстоятельств либо базироваться на оперативно-розыскной информации. Редакция нормы дает довольно широкий простор для усмотрения правоприменительного органа и одновременно ограничивает его

определенными рамками. Следует заметить, что перехват сообщений и снятие информации «на всякий случай» недопустимо. Принимая решение о перехвате сообщений, следователь должен иметь основание предполагать о том, что будет получена информация, «относящаяся к расследуемому делу» (ч. 1 ст. 236 УПК РК). Думается, что здесь идет речь об обстоятельствах, подлежащих доказыванию, так как в противном случае весь массив перехваченной информации будет «относиться к расследуемому делу».

Для выработки цели и определения оснований для производства перехвата сообщений полагаем необходимым обратиться к такому следственному действию как «прослушивание и запись переговоров». Это обусловлено тем, что при перехвате сообщений, также как и при прослушивании переговоров, исследованию подлежит вся информация, проходящая по техническим и компьютерным каналам связи, и во время прослушивания (и перехвата сообщений) невозможно точно установить, что из перехваченной информации будет иметь доказательственное значение.

Редакция ст. 237 УПК РК «Прослушивание и запись переговоров» не определяет целей данного действия, указывая лишь на «наличие достаточных оснований полагать», что при производстве прослушивания будет получена необходимая информация. Хотя, на наш взгляд, при производстве таких действий как перехват и прослушивание, цель позволяет установить границы исследования и использования массива полученной информации. Полагаем, что именно в связи с этим в «Рекомендациях по применению средств видео-, звукозаписи, кинофотоаппаратуры, телефонной связи и использовании полученных результатов при предотвращении, раскрытии и расследовании преступлений» было закреплено, что «прослушивание и звукозапись переговоров производятся для обнаружения, проверки и закрепления фактических данных, имеющих значение доказательств по уголовному делу, с целью:

- выявления лиц, участвовавших в совершении преступления;
- установления мест, где скрываются разыскиваемые преступники,
- выявления места сокрытия похищенного, орудий преступления,
- получения информации об обстоятельствах, подлежащих доказыванию по уголовному делу,
- безотлагательного использования зафиксированных сведений для защиты законных интересов государства и прав граждан» [88].

На основе изложенного и учитывая специфику перехвата сообщений, полагаем необходимым установить пределы исследования и границы вторжения в частную жизнь граждан и интересы учреждений, путем определения цели перехвата сообщений.

Считаем, что целью данного действия является обнаружение информации, передаваемой по техническим, в том числе и компьютерным каналам связи, об обстоятельствах, подлежащих доказыванию по уголовному делу и использования ее при расследовании преступлений. Объектом перехвата сообщений будут являться компьютерная система, компьютерная сеть, технические каналы связи,

исследование которых позволит органу уголовного преследования получить интересующую информацию.

Анализ порядка принятия решения о перехвате сообщений показывает, что единственным основанием для его производства является «постановление следователя, санкционированное прокурором». В данном случае не понятно, что является источником для основания данного решения, чьи сообщения перехватывать (обвиняемых, подозреваемых, свидетелей, потерпевших или других участников уголовного процесса), какие сообщения подлежат перехвату (входящие и (или) исходящие). Полагаем правильным считать, что для определения порядка производства следственного действия и соответственно законности его проведения необходимо наличие не только юридических (постановления) но и фактических (оперативно-розыскная информация, заявления участников уголовного процесса и другие доказательства, полученные по уголовному делу) оснований. Например, при расследовании уголовного дела № 216001 по факту неправомерного доступа в локальную сеть РИВЦ, при допросе один свидетелей (сотрудник РИВЦ) сообщил, что проникнуть в сеть мог их бывший сотрудник, не так давно уволенный с работы и обладающий специальными познаниями в компьютерных технологиях. Проверив данное сообщение, следователем был установлен Н., действительно совершивший данное преступление в отместку за его увольнение с работы [89].

В связи с изложенным, полагаем необходимым более подробно остановиться на рассмотрении оснований для производства перехвата сообщений.

По мнению К. Ж. Капсалямова [90, 64], фактическим основанием для перехвата сообщений являются достаточные данные о том, что в информации, поступающей к конкретному лицу, могут содержаться сведения, имеющие значения для быстрого раскрытия и расследования преступлений, а также своевременного предотвращения готовящихся преступных деяний. Кроме этого, источником для основания перехвата сообщений могут быть данные, полученные в ходе оперативно-розыскных мероприятий, регламентированных ст. 11 Закона РК «Об оперативно-розыскной деятельности» от 12 августа 1995 г. (с изменениями от 10 ноября 2001 г.). Предлагаемые К. Ж. Капсалямовым основания фактически базируются только на понятии «достаточных данных», которое не раскрывается по своему содержанию и является весьма расплывчатым понятием основания.

Хотелось бы остановиться на основаниях, закрепленных в ст. 237 УПК РК и рассмотренных А. Н. Чувилевым, применительно к производству прослушивания переговоров [91, 107]. Исследуя вопросы оснований для прослушивания переговоров, А. Н. Чувилев отмечает, что они сформулированы дифференцированно применительно к двум группам субъектов.

К первой относятся подозреваемые, обвиняемые и иные, причастные к преступлению, лица. Разъяснение относительно того кого следует под ними понимать дано в Рекомендациях по применению средств видео-, звукозаписи кинофотоаппаратуры, телефонной связи и использовании полученных результатов при предотвращении, раскрытии и расследовании преступлений. В п. 14

этого документа сказано, что к иным причастным к преступлению лицам относятся граждане, в отношении которых в деле имеются требующие проверки материалы о том, что они являются участниками преступления либо совершают действия по укрывательству самого преступления, орудий и средств совершения преступления, предметов, добытых преступным путем, либо в иной противоправной форме препятствуют установлению истины по делу [88].

Ко второй группе субъектов, переговоры которых могут прослушиваться и фиксироваться с помощью звукозаписи, отнесены потерпевшие и свидетели.

Прослушивание переговоров, ведущихся по телефону или иным переговорным устройствам потерпевшего либо свидетеля, допускается только при наличии угрозы совершения насилия, вымогательства либо других противоправных действий в отношении этих лиц. Причем обязательным условием правомерности производства данного действия должно быть поступление от потерпевшего или свидетеля соответствующего заявления или их согласие на прослушивание переговоров. Заметим, что заявление об угрозе или согласие может быть сделано и в устной форме. Но, как представляется, его целесообразнее занести в протокол для того, чтобы прокурор, решая вопрос о даче санкции, мог убедиться в наличии для этого оснований.

Таким образом, если прослушивание переговоров первой группы субъектов производится втайне от них, то потерпевший и свидетель всегда об этом осведомлены. Например, в США законодатель даже немного расширил границы правомерности производства прослушивания, закрепив в Законе «О контроле над преступностью и обеспечением безопасности на улицах», что «допускается прослушивание без ордера, если хотя бы один из участников разговора добровольно разрешает сделать это» [86].

Хотелось бы обратить внимание на то, что в УПК ФРГ закреплена статья — «Основания для контроля телефонных переговоров», в которой законодатель устанавливает несколько групп оснований для осуществления контроля и записи переговоров.

В отношении обвиняемого, если определенные факты говорят о том, что:

- кто-либо в качестве исполнителя или соучастника совершил уголовно-наказуемое деяние;
- в случаях, когда покушение наказуемо или он покушался или готовил совершение уголовно-наказуемого деяния;
- если установление обстоятельств дела либо выяснение места нахождения обвиняемого другим способом невыполнимо или существенно затруднено.

В отношении других лиц, о которых на основании определенных фактов известно, что:

- они передают для обвиняемого информацию или от него исходит информация;
- они ее распространяют;
- обвиняемый общается с ними.

Кроме того, в этой же статье закреплено, что контроль может быть установлен по делам об отдельных преступлениях и дает их перечень. В частности, в него включены — преступления против мира, угроза демократическому правовому государству, выдача государственной тайны или угроза внешней безопасности; преступления против публичного порядка, подделка денег или ценных бумаг, похищение людей, убийство, разбой, преступление, предусмотренное законом о наркотиках [92].

Оценивая значимость исследуемой проблемы и учитывая остроту оперативно-розыскных мероприятий по контролю телефонных и иных переговоров, затрагивающих конституционные права человека и гражданина, законодатель Российской Федерации внес дополнительные ограничения на условия проведения таких мероприятий. Теперь в соответствии с ч. 4 ст. 8 Федерального Закона РФ «Об ОРД в РФ» прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях [93]. Соотношение возможности осуществления указанных оперативно-розыскных мероприятий со степенью тяжести противоправного деяния указывает на вынужденный характер их проведения, а также позволяет правоприменителю использовать Особенную часть УК РФ для ограничения конституционных прав граждан [94, 21].

Учитывая больший опыт зарубежных стран, в целях недопущения и устранения пробелов, могущих возникнуть в отечественном законодательстве в связи с особенностями осуществления перехвата сообщений, полагаем необходимым определить перечень отдельных преступлений, при расследовании которых осуществление перехвата сообщений может дать существенный положительный результат для их раскрытия. Данный перечень обусловлен степенью общественной опасности, защитой интересов государства, спецификой совершения данных преступлений (в частности, возможностью использования современных средств связи при их подготовке и совершении), не является окончательным и может быть расширен законодателем.

В качестве рекомендаций предлагается использование перехвата сообщений при расследовании преступлений, предусмотренными следующими статьями Уголовного кодекса Республики Казахстан:

Преступления против правосудия — ст. 339 УК РК «Воспрепятствование осуществлению правосудия и производству предварительного следствия», ст. 341 УК РК «Угроза или насильственные действия в связи с осуществлением правосудия или производством предварительного расследования», ст. 347 УК РК «Принуждение к даче показаний», ст. 354 УК РК «Подкуп или принуждение к даче ложных показаний …», ст. 356 УК РК «Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса», ст. 358 УК РК «Побег из мест лишения свободы, из-под ареста или из-под стражи», ст. 363 УК РК «Укрывательство преступления», ст. 364 УК РК «Недонесение о преступлении».

Воинские преступления — ст. 386 УК РК «Разглашение военной тайны …».

Преступления против общественной безопасности и общественного порядка — ст. 233 УК РК «Терроризм», ст. 234 УК РК «Захват заложника», ст. 235 УК РК «Создание и руководство организованной преступной группой или преступным сообществом, участие в преступном сообществе», ст. 236 УК РК «Организация незаконного военизированного формирования», ст. 237 УК РК «Бандитизм», ст. 238 УК РК «Захват зданий, сооружений, средств сообщения и связи», ст. 243 УК РК «Незаконный экспорт технологий, научно-технической информации …», ст. 252 УК РК «Незаконное изготовление оружия»

Преступления против основ конституционного строя и безопасности государства — ст. 166 УК РК «Шпионаж», ст. 168 УК РК «Насильственный захват власти или насильственное удержание власти», ст. 172 УК РК «Разглашение государственной тайны»

Преступления против мира и безопасности человечества — ст. 156 УК РК «Планирование, подготовка, развязывание или ведение агрессивной войны».

Преступления против конституционных и иных прав и свобод человека и гражданина — ст. 142 УК РК «Нарушение неприкосновенности частной жизни», ст. 143 УК РК «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений».

Преступления против семьи и несовершеннолетних — ст. 133 УК РК «Торговля несовершеннолетними».

Подводя итог рассмотрению вопроса о фактических основаниях производства следственного действия, следует констатировать, что их закрепление в нормах Уголовно-процессуального кодекса РК позволит регламентировать порядок производства, установит гарантии правомерности производства следственного действия. На основании изложенного предлагается дополнить ст. 236 УПК РК частями следующего содержания:

1. Перехват сообщений и снятие с компьютерных систем информации производится на основании фактических данных, дающих основание полагать, что в информации, поступающей и отправляемой подозреваемым, обвиняемым, могут содержаться сведения, имеющие значение для дела, а также для своевременного предотвращения готовящихся преступных деяний.
2. Перехват сообщений потерпевшего, свидетеля и других участников уголовного процесса допускается при наличии угрозы совершения насилия, вымогательства либо других противоправных действий в отношении этих лиц на основании соответствующего заявления или с их согласия на перехват сообщений.
3. Перехват сообщений свидетелей, потерпевших, других участников уголовного процесса допускается без их согласия при наличии информации о том, что они совершают действия по укрывательству преступления, орудий и средств совершения преступления, предметов, добытых пре-

ступным путем, препятствуют установлению истины по делу, обмениваются информацией с подозреваемым, обвиняемым.

Рассмотрев фактические основания электронного прослушивания, полагаем необходимым остановиться и на условиях назначения и проведения данного действия. По мнению Ю. М. Батурина, А. М. Жодзишского, при назначении прослушивания должно существовать достаточное основание предполагать, что конкретное преступление совершено или совершается, и доказательства этого будут получены путем подслушивания. Кроме того, ими предлагаются и следующие условия: «разговоры, которые планируется перехватить, должны быть четко обозначены в ордере; прослушивание должно быть ограничено во времени; продление может быть разрешено только при новом представлении достаточного основания; прослушивание должно быть прекращено, как только искомые доказательства получены; запрос на выдачу ордера должен быть представлен в письменной форме, за исключением безотлагательных ситуаций; ордер должен быть возвращен по исполнении с детальным описанием перехваченных разговоров» [33, 124].

Думается, что отдельные условия будут применимы и к перехвату сообщений. Учитывая специфику перехвата сообщений и рассмотренные выше мнения ученых, предлагается выделить следующие условия:

- специфика сообщений, которые планируется перехватить, должна быть четко обозначена в постановлении (входящие и (или) исходящие);
- перехват сообщений может носить разовый или продолжительный характер;
- перехват сообщений должен быть ограничен во времени;
- продление первоначального срока перехвата сообщений производится на основании нового постановления следователя, санкционированного прокурором;
- перехват сообщений производится с санкции прокурора, за исключением безотлагательных ситуаций (на основе оперативно-розыскной информации, заявления участников процесса);
- сообщения и компьютерная информация, полученные в результате перехвата, фиксируются специалистом на соответствующем носителе и передаются следователю в опечатанном виде с указанием даты и времени перехвата;
- после получения перехваченных сообщений следователь обязан просмотреть информацию и решить вопрос о ее судьбе.

Рассматривая вопрос юридического основания перехвата сообщений, отмечаем, что согласно ст. 236 УПК РК, основанием для производства перехвата сообщений является постановление следователя, санкционированное прокурором. Между тем, полагаем, что перечень лиц, имеющих право назначить перехват сообщений, должен быть расширен. Так, прокурор, осуществляя надзор за законностью оперативно-розыскной деятельности, дознания, следствия, а также и уголовное преследование, согласно п. 2 ч. 1 ст. 197 УПК РК имеет право дать

письменное указание о производстве следственных действий, которое является обязательным для исполнения сотрудниками дознания и следствия. Следовательно, решение прокурора о назначении перехвата сообщений является обязательным для исполнения и входит в категорию юридических оснований для его производства.

Кроме того, подвергая анализу санкционирование доступа к компьютерным сетям мы видим, что законодатель не указывает категории лиц, дающих разрешение на проникновение в системы связи и проведение следственных мероприятий. Полагаем, следует учитывать, что в зависимости от вида системы (глобальная, локальная), в которую необходимо проникнуть и распределения подключенных к ней терминалов, может изменяться статус прокурора, санкционирующего данное действие. Например, санкция перехвата сообщений абонентов в пределах населенного пункта дается районным, городским прокурором или их заместителями; в пределах области или территории Республики Казахстан — прокурорами областей и приравненных к ним прокурорами.

Таким образом, прежде чем приступить к производству данного следственного действия необходимо вынести мотивированное постановление, которое должно быть санкционировано прокурором.

Постановление следователя о производстве перехвата сообщений должно содержать основание, которое послужило для перехвата сообщения, данные о лице (организации) — чьи сообщения подлежат перехвату. Кроме того, при наличии соответствующей информации, необходимо указать также вид канала связи либо компьютерной системы, которая должна контролироваться и срок контроля.

Постановление следователя, санкционированное прокурором, направляется для исполнения органу, осуществляющему оперативно-розыскную деятельность. Так как для перехвата сообщений на различных технических носителях необходимы специальные познания, то он производится обязательно при техническом содействии соответствующего специалиста. Следует обратить внимание, что если оперативным подразделением для производства перехвата привлекался специалист, не являющийся сотрудником правоохранительных органов, его необходимо предупредить об ответственности за разглашение ставших известных ему сведений, в соответствии со ст. ст. 53, 205 УПК РК. Рекомендуемый способ исполнения решения следователя о перехвате сообщений удобен, поскольку не требует от него каких-либо других усилий, перекладывая всю технологию прослушивания на плечи органа дознания и специалиста.

В настоящее время практикой не выработан единый путь привлечения специалиста к участию в следственных действиях или производству каких-либо действий — в одних случаях специалист вызывается повесткой, в других, например, при расследовании уголовного дела № 030710 необходимость исследования специалистом программного обеспечения, диагностики отдельных программ и осмотра содержимого компьютера следователем была решена путем дачи отдельного поручения.

В то же время предлагается и другой способ, который, по нашему мнению, требует закрепления в законе. Санкционированное прокурором постановление направляется для исполнения администрации телефонного узла, телефонной станции, провайдеру. Такой порядок представляется предпочтительным в случаях, когда перехват сообщений носит не одноразовый характер, а должен осуществляться довольно длительное время. Если неизвестно, когда последует интересующая следователя информация, его ожидание требует отвлечения работников органа дознания от исполнения других обязанностей, что вряд ли реально. Поэтому целесообразно предусмотреть в УПК право следователя поручать прослушивание органу дознания либо узлу телефонной связи или провайдеру. Изложенные положения нашли свое подтверждение в отзывах сотрудников органов прокуратуры по исследуемым вопросам (см. Приложение Г).

В качестве примера содержания резолютивной части постановления о перехвате сообщений предлагается выдержка из образца, разработанного автором:

«ПОСТАНОВИЛ:

1. Произвести перехват сообщений, получаемых по компьютерному каналу связи, адрес электронной почты “rotary@rrr.kaz”, подключенного к компьютеру находящемуся по адресу: г. К., ул. Гоголя, 45-44.

2. Производство перехвата сообщений по компьютерному каналу связи и их запись поручить специалистам ОАО “Казахтелеком”.

3. В соответствии с требованиями ст. ст. 53 и 205 УПК РК разъяснить руководителю и специалистам ОАО “Казахтелеком”, осуществляющим перехват сообщений, о сохранении конфиденциальности.

4. Предупредить руководителя и специалистов ОАО “Казахтелеком”, осуществляющим перехват сообщений, об уголовной ответственности по ст. 355 УК РК за разглашение данных предварительного расследования» [95].

Кроме того, полагаем, что в постановлении должно быть указано время передачи перехваченной информации следователю. Передача может осуществляться по истечении определенного времени (например, каждые 3 дня, каждый понедельник) или при перехвате каждого сообщения.

На основании рассмотренных выше положений, понятия и содержания структурных элементов перехвата сообщений, как самостоятельного следственного действия, предлагаются следующие определения и выводы.

Целью перехвата сообщений является обнаружение информации, передаваемой по техническим, в том числе и компьютерным каналам связи об обстоятельствах, подлежащих доказыванию по уголовному делу, и использование ее при расследовании преступлений.

Объектом перехвата сообщений являются компьютерная система, компьютерная сеть, технические каналы связи.

К условиям производства перехвата сообщений относятся:

- специфика сообщений, которые планируется перехватить, должна быть четко обозначена в постановлении (входящие и (или) исходящие);
- разовый или продолжительный характер перехвата сообщений;

– время проведения перехвата сообщений, которое должно быть по возможности ограничено;
– необходимость продления первоначального срока перехвата сообщений, которое производится на основании нового постановления следователя, санкционированного прокурором;
– необходимость санкции прокурора, за исключением безотлагательных ситуаций (на основе оперативно-розыскной информации, заявления участников процесса);
– участие специалиста;
– решение вопроса о судьбе перехваченных сообщений.

Субъектами, имеющими право назначать перехват сообщений, являются прокурор, следователь, дознаватель.

В зависимости от вида системы (глобальная, локальная), в которую необходимо проникнуть и распределения подключенных к ней терминалов, может изменяться статус прокурора, санкционирующего данное действие. Например, санкция перехвата сообщений абонентов в пределах населенного пункта дается районным, городским прокурором или их заместителями; в пределах области или территории Республики Казахстан — прокурорами областей и приравненных к ним прокурорами.

Перехват сообщений, передаваемых с технических, в том числе компьютерных каналов связи, осуществляется при наличии фактических (оперативно-розыскная информация, заявления участников уголовного процесса и другие доказательства, полученные по уголовному делу) и юридических (постановления) оснований.

В соответствии с данными положениями предлагаются следующие изменения и дополнения, направленные на совершенствование законодательной регламентации перехвата сообщений.

Часть 1 ст. 236 УПК РК предлагается изложить в следующей редакции:

«1. Перехват сообщений, передаваемых по техническим в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации, относящейся к расследуемому делу, производятся на основании постановления следователя, санкционированного прокурором с целью получения информации об обстоятельствах, подлежащих доказыванию по уголовному делу и использовании ее для установления объективной истины.

Постановление следователя о производстве перехвата сообщений должно содержать номер уголовного дела и основания, по которым должно производиться данное действие, данные о лице (организации) — чьи сообщения подлежат перехвату. В постановлении должны быть указаны сроки передачи изымаемой информации или сообщения об отсутствии передаваемой и (или) получаемой абонентом компьютерной информации. При наличии соответствующей информации необходимо указать также вид канала связи либо компьютерной системы, которая должна контролироваться».

Изложить ч. 2 ст. 236 УПК РК в следующей редакции: «Постановление следователя, санкционированное прокурором, направляется для исполнения ор-

гану, осуществляющему ОРД или администрации телефонного узла, телефонной станции, организациям и учреждениям, осуществляющих предоставление услуг по работе в компьютерных сетях».

Дополнить ст. 236 УПК РК частью следующего содержания: «Санкция на перехват сообщений абонентов в пределах населенного пункта дается районным, городским прокурором или их заместителями; в пределах области или территории Республики Казахстан — прокурорами областей и приравненных к ним прокурорами».

Изложить ч. 3 ст. 236 УПК РК в следующей редакции: «Сообщения и компьютерная информация, полученные в результате перехвата, фиксируются специалистом на соответствующем носителе и передаются следователю в опечатанном виде с указанием даты, времени перехвата и краткой характеристики использованных при этом технических средств».

2.3 Процессуальный порядок и сроки производства перехвата сообщений

Анализируя различные аспекты деятельности правоохранительных органов в сфере уголовного судопроизводства, прежде всего, следует акцентировать внимание на установленных уголовно-процессуальным законом промежутках времени, в течение которых должны или могут быть совершены определенные действия, предусмотренные нормами кодекса и характеризующиеся процессуальными сроками.

Правильное исчисление процессуальных сроков, будучи условием их строгого и точного соблюдения, имеет важное правовое значение. Следует помнить, что соответственно наступление или истечение процессуального срока обычно выступает в качестве необходимого юридического условия для правомерного применения закона. Ошибки в исчислении процессуальных сроков могут стать (и нередко становятся) одной из причин неправильного применения закона, нарушения прав и законных интересов граждан, вовлекаемых в уголовный процесс и, следовательно, в конечном итоге несоблюдения важнейших интересов правосудия.

Правовые нормы (а равно базирующиеся на их основе нормативные правовые акты) устанавливают не только «что» и «как» нужно сделать, но и «в какие сроки». Поэтому процессуальные сроки — зачастую необходимый, обязательный элемент правила поведения соответствующего субъекта (участника) процесса. Иначе говоря, сроки нередко составляют один из элементов диспозиции правовой нормы. В силу правового характера процессуальных сроков их правильное исчисление и соблюдение обеспечивается силой государственного принуждения. Это обусловлено тем, что точное исполнение и соблюдение процессуальных сроков обеспечивает успешное решение задач уголовного судопроизводства, так как нарушение сроков может повлечь отмену процессуальных решений либо утрату участником процесса своего процессуального права. За нарушение указанных сроков виновные могут быть подвергнуты мерам дис-

циплинарного и административного наказания. Если же допускаемое нарушение (например, сроков задержания или ареста) — результат преступного злоупотребления соответствующим должностным лицом, ведущим процесс, властью или служебным положением, либо преступного превышения власти или служебных полномочий, либо преступной должностной халатности, может наступить и уголовная ответственность по соответствующим статьям уголовного закона.

Только при правильном исчислении установленных законом сроков, своевременном реагировании органов дознания, следствия, прокурора и суда на случаи совершенных и подготовляемых преступлений, быстром и полном их раскрытии и расследовании можно достаточно прочно гарантировать соблюдение законных интересов государства, общества и личности, обеспечить их оптимальное соотношение и развитие. Между тем, специфичность деятельности правоохранительных органов неразрывно связана с применением различного вида мер принуждения и ограничением прав граждан, в связи с возложенной на них обязанностью раскрытия и расследования преступлений. Ограничение неприкосновенности частной жизни в области тайны сообщений, передаваемых по компьютерным и техническим каналам связи, являются одним из аспектов данной деятельности. Актуальность охраны и защиты частной жизни граждан связана с использованием ими достижений технологического прогресса при общении между собой и ведении личных записей, которые, исходя из целей уголовного судопроизводства, подвергаются исследованию правоохранительными органами. Особенности и пределы ограничения принципа неприкосновенности побудили нас к рассмотрению данной проблемы в свете осуществления органом уголовного преследования перехвата сообщений, передаваемых с компьютерных и технических каналов связи.

В условиях постоянно развивающейся технологии подслушивания и перехвата информации, защита частной жизни граждан требует большего, чем простой запрет, необоснованного физического нарушения владения и изъятия материальных предметов. Таким образом, единственным подходом к сдерживанию негативных проявлений научно-технической революции является выработка стандартов и создание процедур, гарантирующих право на частную жизнь. Введение в Уголовно-процессуальный кодекс ст. 236 «Перехват сообщений» является первым шагом государства (в технологической сфере процессуального направления), направленным на реализацию положений ст. 18 Конституции РК, закрепляющих право каждого на «неприкосновенность частной жизни, личную и семейную тайны, право на тайну переписки, телефонных переговоров и иных сообщений», и определение процедуры «ограничения этого права в случаях и в порядке, прямо установленных законом» [77].

Между тем, необходимо отметить, что перехват сообщений и снятие информации с компьютерных систем, являясь грозным орудием вторжения государства в частную жизнь граждан, не был определен в сроках получения и использования информации. Большие затруднения на практике вызывает вопрос о продолжительности данных действий — необходимо ли получать санкцию

прокурора каждый раз перед проведением данного следственного действия, либо единожды по уголовному делу, каков первоначальный и общий срок его проведения.

Анализируя процессуальное законодательство зарубежных стран, в частности, России, Германии, США в сфере контроля и записи переговоров и иных сообщений, мы видим, что в каждом государстве установлены различные сроки производства данного действия.

Так, в ч. 5 ст. 186 «Контроль и запись переговоров» УПК Российской Федерации установлено: «Производство контроля и записи телефонных и иных переговоров может быть установлено на срок до 6 месяцев. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу» [96].

В ч. 2 ст. 99 УПК ФРГ «Компетентный орган контроля за телефонными переговорами» закреплено, что предписание о контроле и записи переговоров должно содержать «вид, объем и срок производимых действий. Максимальный срок действия предписания — три месяца. Продление допускается не более чем на три месяца, если на то имеются основания» [92].

В Законе США «О контроле над преступностью и обеспечением безопасности на улицах» третьим разделом, озаглавленным «Подслушивание телефонных переговоров и электронное прослушивание», установлено, что «ордер на подслушивание выдается на срок до 30 дней. Он может быть в исключительных случаях продлен, но не более чем на 30 дней» [86]. Ряд американских юристов, при общей положительной оценке нового закона, в настоящее время высказывают ряд соображений об уточнении некоторых понятий и введении определенных ограничений. Прежде всего, речь идет о сокращении как минимум вдвое 30-дневного срока прослушивания (даже без учета продления). Столь длительный срок считается нецелесообразным с практической точки зрения и слишком серьезным с точки зрения вторжения в личную жизнь. Во-вторых, предлагается установить жесткий судебный контроль за проводимым подслушиванием. В настоящее время такой контроль законодательно на уровне штатов не предусмотрен (в федеральной системе этот срок составляет 10 дней).

Приведенные выше примеры позволяют констатировать тот факт, что продолжительность перехвата сообщений зависит от специфики уголовного процесса государства и приоритетности норм, определяющих защиту частной жизни граждан и задач уголовного судопроизводства. Исходя из данной позиции и учитывая, что Конституция Республики Казахстан (ст. 1) утверждает высшими ценностями государства человека, его жизнь, права и свободы, полагаем необходимым установить (в ст. 236 УПК РК) срок перехвата сообщений до двух месяцев. То есть в пределах первоначального срока, установленного для производства предварительного следствия, «обусловленного экономией использования процессуальных средств, и определенного из соображений целесообразности для обеспечения всестороннего, полного и объективного исследования всех обстоятельств преступного деяния» [97, 257].

Дальнейшее продление первоначального срока производства перехвата сообщений, полагаем, должно соотноситься с положениями ст. 196 УПК РК «Срок предварительного следствия», определяющими основания и порядок продления сроков расследования уголовного дела. Считаем, что обстоятельства, послужившие основанием для продления срока перехвата сообщений и ожидаемые результаты его производства, могут быть указаны в составляемом следователем постановлении о продлении сроков следствия, наряду с основными положениями, обуславливающими необходимость продления сроков расследования, либо в отдельном постановлении. Санкционирование данного решения производится прокурорами в соответствии с положениями ч. ч. 4, 5 ст. 196 УПК РК.

Кроме изложенного выше «продолжительного» срока, полагаем, что перехват сообщений может носить «разовый» характер, который характеризуется возможностью уменьшения сроков его проведения и обуславливается следующим:

- в случаях, когда следствие интересует возможность получения или отправления лицом, с использованием компьютерной техники различных сообщений, перехват сообщений назначается с целью установления данного аспекта. Несомненно, определяемую возможность можно установить и в ходе следственного эксперимента, но данный случай связан с той ситуацией, когда в силу определенных обстоятельств это затруднительно (например, наличие паролей доступа и идентификации) или обусловлено оперативно-следственной необходимостью;
- в случаях, когда перехват сообщений производится до получения интересующей следствие информации и следствию известны сроки ее передачи (на основе заявлений участников уголовного процесса, оперативно-розыскной информации и другого).

В обозначенных выше случаях следователь, составляя постановление о производстве перехвата сообщений, указывает границы проводимого действия и обозначает специфичность его производства, определяя, таким образом, направленность действий специалистов, осуществляющих перехват, экономя время и улучшая качество получаемых результатов.

При расследовании уголовного дела в форме дознания, действуют установленные выше сроки, за исключением того, что «продолжительный» срок перехвата сообщений будет ограничиваться тридцатисуточным сроком в соответствии со ст. 285 УПК РК. Производство же перехвата сообщений в 10-дневный срок будет носить «разовый» характер и необходимость его назначения должно определяться указанными обстоятельствами.

Приостановление предварительного следствия (в порядке, установленном ст. 265 УПК РК) влечет за собой приостановление перехвата сообщений с технических каналов связи и компьютерных систем, о чем может быть указано в постановлении «о приостановлении предварительного следствия» или в отдельном постановлении «о приостановлении производства перехвата сообщений». Приостановление перехвата сообщений также может быть обусловлено:

помещением лица, чьи сообщения перехватываются, на стационарное лечение в лечебные учреждения в связи с заболеванием, указанием прокурора и другим.

Производство перехвата сообщений прекращается по постановлению следователя, дознавателя, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу. Прекращение производства перехвата сообщений может быть осуществлено прокурором на основании его полномочий и в порядке, определенных положениями Уголовно-процессуального кодекса.

Возобновление производства перехвата сообщений производится на основании положений ч. 1 ст. 268 УПК РК или наряду с возобновлением предварительного следствия. При вынесении органом уголовного преследования постановления о возобновлении предварительного следствия в этом же документе может быть указано и о возобновлении производства перехвата сообщений. При этом, как в отдельно выносимом постановлении о возобновлении производства перехвата сообщений, так и в постановлении о возобновлении предварительного следствия должно быть указано — сохраняется ли прежний режим перехвата сообщений (продолжительный, с установленными сроками отчетности) или же если вносятся изменения, указать их специфику.

На основании проведенного выше анализа и исследования особенностей производства перехвата сообщений предлагаются следующие выводы и положения.

Перехват сообщений, передаваемых по техническим, в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации может носить «продолжительный» и «разовый» характер.

«Продолжительный» вид перехвата сообщений устанавливается до двух месяцев — в пределах первоначального срока, установленного для производства предварительного следствия. Дальнейшее продление первоначального срока производства перехвата сообщений осуществляется в соответствии с положениями ст. 196 УПК РК «Срок предварительного следствия», определяющими основания и порядок продления сроков расследования уголовного дела. Обстоятельства, послужившие основанием для продления срока перехвата сообщений и ожидаемые результаты его производства, могут быть указаны в составляемом следователем постановлении о продлении сроков следствия, наряду с основными положениями, обусловливающими необходимость продления сроков расследования, либо в отдельном постановлении. Санкционирование данного решения производится прокурорами в соответствии с положениями ч. ч. 4, 5 ст. 196 УПК РК.

«Разовый» вид перехвата сообщений характеризуется возможностью уменьшения сроков его проведения и обусловливается следующими обстоятельствами:

1. В случаях, когда следствие интересует возможность получения или отправления лицом с использованием компьютерной техники различных сообщений, перехват сообщений назначается с целью установления данного вопроса.

2. В случаях, когда перехват сообщений производится до получения интересующей следствие информации и следствию известны сроки ее передачи (на основе заявлений участников уголовного процесса, оперативно-розыскной информации и другого).

При расследовании уголовного дела в форме дознания действуют установленные выше сроки, за исключением того, что «продолжительный» срок перехвата сообщений будет ограничиваться тридцатисуточным сроком в соответствии со ст. 285 УПК РК. Производство же перехвата сообщений в 10-дневный срок будет носить «разовый» характер и необходимость его назначения должна определяться указанными обстоятельствами.

Предлагается дополнить ст. 236 УПК РК частями следующего содержания:

«Перехват сообщений, передаваемых по техническим, в том числе, и компьютерным каналам связи, и снятие с компьютерных систем информации устанавливается на срок до двух месяцев. Дальнейшее продление срока производится в соответствии с положениями ч. ч. 4, 5, 6, 7 ст. 196 УПК РК.

О приостановление перехвата сообщений указывается в постановлении о приостановлении предварительного следствия или в отдельном постановлении «о приостановлении производства перехвата сообщений», вынесенном следователем, дознавателем, прокурором.

Производство перехвата сообщений прекращается по постановлению следователя, дознавателя, прокурора, если необходимость в данной мере отпадает, но не позднее окончания расследования по данному уголовному делу.

Возобновление производства перехвата сообщений производится на основании положений ч. ч. 1, 2 ст. 268 УПК РК или наряду с возобновлением предварительного следствия. В постановлении должно быть указано — сохраняется ли прежний режим перехвата сообщений или изменяется. Установленные изменения указываются в выносимом постановлении».

2.4 Иные методы и способы обнаружения и закрепления информации при перехвате сообщений

На эффективность работы в борьбе с преступлениями в сфере высоких технологий оказывает влияние то обстоятельство, что «далеко не всегда следователи, приступая к производству расследования по делам о таких преступлениях, представляют себе особенности собирания доказательств в компьютерных сетях» [98, 15]. Данное обстоятельство требует уяснения основных особенностей таких следов и работы с ними. Прежде всего, необходимо учитывать, что компьютерная информация легко передается, копируется, блокируется или модифицируется с беспрецедентной скоростью на значительном от нее расстоянии. Это свойство обусловлено самой природой компьютерной информации, которая может являться, с одной стороны, носителем следов, а с другой — следами совершенных преступлений. Для таких следов характерны «специфические свойства, определяющие перспективы их регистрации, извлечения и использования в качестве доказательств, при расследовании совершенного пре-

ступления. Во-первых, “виртуальные следы” существуют на материальном носителе, но не доступны непосредственному восприятию. Для их извлечения необходимо обязательное использование программно-технических средств. Они не имеют жесткой связи с устройством, осуществившим запись информации, являющейся “виртуальным следом”, весьма неустойчивы, так как могут быть легко уничтожены. Во-вторых, получаемые “виртуальные следы” внутренне ненадежны (благодаря своей природе), так как их можно неправильно считать» [99, 74].

Но, несмотря на указанные особенности, следы преступлений, совершенных с использованием компьютерных сетей, могут быть обнаружены в сведениях о прохождении информации (они включают в себя название источника сообщения, его назначение, маршрут, время, дату, продолжительность, характер деятельности при сообщении и место назначения) по проводной, радиооптической и другим электромагнитным системам связи. В специальной литературе и документах сведения о прохождении информации именуются как «сведения о сообщениях, передаваемых по сетям электрической связи (электросвязи)», либо сохраняемые поставщиками услуг (провайдерами) «исторические данные» о состоявшихся сеансах связи или переданных сообщениях, либо «данные о потоках» или «данные о потоках информации». В принципе, все эти определения являются синонимами [100, 12].

Указанные сведения о сообщениях, передаваемых по сетям электросвязи, аккумулируются в специальных файлах регистрации — LOG-файлах. В большинстве компьютерных систем ведение файлов регистрации — часть повседневной деятельности. Когда бы событие определенного рода ни произошло в системе, информация о нем (в том числе кто инициировал его, когда и в какое время оно произошло, и если при этом были затронуты файлы, то какие) регистрируется в данных файлах. То есть, по существу, в них протоколируется техническая информация, содержатся данные о техническом обмене. В силу этого их порой упоминают как «регистрационный журнал».

Принципиально существует две основные категории «исторических данных»: данные о пользователе и сведения о сообщении. Раскрывая данные категории, полагаем необходимым обратиться к работе А. Г. Волеводз, в которой достаточно полно и ясно изложены интересующие нас сведения. Так, «данные о пользователе могут включать: имя, адрес, дату рождения, номер телефона, адрес поставщика услуг в Internet, адрес электронной почты, идентификационные признаки какого-либо номера или счета, используемых для осуществления платежных операций по расчетам за услуги провайдера, справочные данные, идентификационные данные юридического лица, перечень предоставляемых услуг или услуг, на которые подписался клиент, IP-адрес (представляет собой уникальный 32-битный адрес каждого компьютера в сети Internet), предыдущий IP-адрес пользователя, дополнительный адрес электронной почты и т. д.

Сведения о сообщении могут включать: первоначальный номер телефона, используемый для связи с LOG-файлом регистрации, дату сеанса связи, информацию о времени связи (времени начало, окончания и продолжительность сеан-

са связи), статические или динамические IP-адресные журналы регистрации провайдера в Internet и соответствующие телефонные номера, скорость передачи сообщения, исходящие журналы сеанса связи, включая тип использованных протоколов, сами протоколы и т. д. Из приведенного перечня видно, что их значение для установления истины при расследовании преступлений неодинаково» [101, 4-54].

Обычно сохранение незначительной доли «исторических данных» осуществляется провайдерами для целей осуществления контроля поступающих за их услуги платежей. Однако в большинстве стран отсутствуют единые стандарты их накопления и сохранения. Зачастую коммерческие службы, доступные в Internet, предусматривают анонимность как услугу. Поскольку многие системы позволяют изменять конфигурацию файлов регистрации (включать и исключать различные виды регистрируемых событий, задавать только определенные виды регистрируемых событий, определять устройства, на которых желательно их вести) — соответствующие провайдеры свободно удаляют на международном уровне всю идентификационную информацию из LOG-файлов, не допуская установления личности отправителя. Это происходит по той причине, что назначение файлов регистрации не заключается в предупреждении и пресечении преступной деятельности — они просто записывают действия системы.

Например, запись в файл регистрации может осуществляться, в случаях, когда: пользователь входит или пытается войти в систему; открывает файл или пытается открыть один из файлов, для доступа к которым он не имеет соответствующих полномочий; пользователь запускает программу, которая преодолевает средства защиты системы, либо экспортирует данные в устройство, находящееся за пределами конкретной сети, и так далее. Форматы и объемы данных в регистрационных файлах зависят от возможностей операционной системы и сетевых соединений. Высокозащищенные системы могут включать в них большое количество дополнительной информации, которая регистрируется в соответствии с установками системных администраторов.

В качестве примера возможности использования анализа LOG-файлов при расследовании преступлений и положительном результате их исследования, приведем выдержки из материалов уголовного дела № 216001 по факту неправомерного доступа в локальную сеть. Так, расследуя данное преступление, следователем была назначена судебно-технологическая экспертиза и представлены на исследование LOG-файлы серверов. Проведенным исследованием установлено: «что 13.07.01 и 16.07.01 на сервере удаленно запускались команды dir (просмотр), del (удаление), type (вывода на экран), format (форматирование). Команды запускались с машины, находящейся в бухгалтерии ШЧ-5 и имеющей сетевой адрес 192.169.19.3. также установлено, что с машины, имеющей сетевой адрес 192.168.49.74 и расположенной в здании РИВЦ тоже запускались команды просмотра (dir), вывода на экран (type) и копирование файла default [htm на PROXY-сервер. Ниже приводится точное время запуска вышеуказанных программ, а также сетевой адрес компьютера, с которого они запускались:

– 192.169.19.3 — адрес компьютера в сети, с которого запускалась команда;
– 167.07.01, 18:02:10 — дата и время запуска команды;
– /scripts/.%5c..%cwinnt /system32 /cmd.exe,/c+del+c:\winnt\syste32\win.com — запуск команды удаления (del);
– /scripts/.%5c..%cwinnt /system32 /cmd.exe, /c+dir+d:\ — запуск команды чтения содержимого каталогов (dir);
– /scripts/.%5c..%cwinnt /system32 /format.com+c:+\ — запуск команды format.

Выводы:

1. Несанкционированный доступ к серверу Primary происходил с компьютера, имеющего сетевой адрес 192.169.19.3 и расположенного в бухгалтерии ЩЧ-5 в следующей последовательности: сканирование каталогов, удаление файлов.
2. Несанкционированный доступ производился:

13.07.01 с 10:20:47 до 11:46:36 и с 13:09:16 до 17:13:07.
16.07.01 с 08:24:31 до 08:40:43 и с 16:47:50 до 18:06:10.

3. Копирование файла default.html с текстом «XXX» было произведено с компьютера, имеющего сетевой адрес 192.168.49.74 и расположенного в здании РИВЦ в кабинете 308» [90].

Кроме LOG-файлов носителями доказательственной информации могут являться и иные «виртуальные следы», остающиеся в компьютерах, используемых для совершения преступных действий либо через которые проходит или поступает информация. Такими носителями, в зависимости от существа действий с информацией, могут являться: таблицы размещения файлов (FAT, NTFS или другие), системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное.

В отличие от LOG-файлов информация, содержащаяся в этих и иных носителях, является достаточно разрозненной, представлена зачастую в несистематизированном виде, что затрудняет деятельность по ее обнаружению, закреплению, изъятию, сохранению и исследованию.

В силу этого LOG-файлы (и соответственно сохраняемые ими сведения о сообщениях, передаваемых по сетям электросвязи) следует признать наиболее значимыми носителями следовой информации о совершении преступлений в компьютерных сетях.

В связи с изложенным, желательным было бы сохранение LOG-файлов провайдерами в своеобразных электронных архивах. Наподобие того, как, к примеру, в архивах кредитно-финансовых учреждений длительные периоды времени хранятся документы о платежных операциях и лицах, их совершивших. При необходимости с соблюдением установленной законом процессуальной формы они могли бы передаваться представителям органов дознания или

предварительного следствия для целей, связанных с расследованием преступлений.

Полагаем необходимым привести в качестве примера, возможность решения данного вопроса законодательством США, в котором предусмотрена возможность направления «запроса о сохранении улик преступления». Согласно §2703 (f) (2) Титула 18 Свода законов США, в соответствии с таким запросом телекоммуникационные службы и Internet-провайдеры обязаны по запросу правительственных учреждений и органов принять все необходимые меры к сохранению данных или других свидетельств, имеющихся в их распоряжении, до издания судом соответствующего судебного приказа, на основе которого эти данные изымаются в распоряжение органов правосудия. Компетентные органы вправе получить запрашиваемые данные в течение срока их хранения, а именно на протяжении 180 дней [102, 897].

Продолжая исследование вопроса обнаружения и фиксации следов в компьютерных сетях, отметим, что информация, которую содержат LOG-файлы (файлы регистрации), может оказаться весьма полезной, так как несет в себе следы преступлений, совершенных с использованием компьютерных сетей. Следовательно, для успешного собирания доказательств таких преступлений требуется своевременно обеспечить обнаружение, изъятие и сохранение имеющихся сведений о сообщениях, передаваемых по сетям электрической связи.

Реализация предоставляемых действующим уголовно-процессуальным законодательством возможностей собирания доказательств при расследовании преступлений в сфере компьютерной информации сталкивается с рядом существенных трудностей и проблем, одной из которых является розыск компьютерной информации. При раскрытии и расследовании преступлений в сфере компьютерной информации зачастую возникает необходимость не столько в получении «исторических данных» или отслеживании сообщений, передаваемых по сетям электросвязи, в реальном масштабе времени, сколько в поисковой деятельности, направленной на установление (и лишь затем изъятие) компьютерной информации при наличии достаточных оснований полагать, что она имеет существенное значение для установления истины по уголовному делу.

Развитие средств телекоммуникаций и обеспечение правоохранительных органов соответствующими аппаратно-программными средствами технически позволяет «проходить» в глобальных сетях по «следам» сообщений, передаваемых по сетям электросвязи, последовательно от сервера к серверу, от компьютера к компьютеру, для их отыскания и изъятия.

Если сопоставить механизмы такой деятельности с общеизвестными уголовно-процессуальными институтами, то мы можем условно обозначить ее как розыск в компьютерных сетях (или в среде для хранения компьютерных данных) с целью обнаружения и изъятия искомой компьютерной информации.

От обычного такой розыск отличается тем, что:

– он может проводиться с использованием удаленного компьютерного терминала;

– в силу объективных причин, связанных с прохождением информации посети, состоящей из множества носителей информации, он затронет не только разыскиваемую компьютерную информацию, но и иную, не имеющую какого-либо отношения к розыску (по преимуществу находящуюся в распоряжении поставщиков услуг).

В качестве примера реальной возможности осуществления розыска искомой информации приведем выступление эксперта по компьютерной безопасности Френка Кили. Вместе с журналистом он исследовал защищенность беспроводных сетей и работу модемов нового класса изготовляемых фирмой «Agere Systems» и компанией «Linksys». Находясь в машине и имея при себе PC-карту для беспроводных сетей, антенну, смонтированную на крыше автомобиля, он за полчаса получил доступ к более 40 беспроводным сетям в частных домах, агентствах, офисах и даже в одном банке. При этом он имел возможность путешествовать по Интернету за чужой счет, создавать учетные записи Hotmail, посылать сообщения по электронной почте (при этом источник отправления определить не удастся), просмотреть имеющуюся информацию, удалить файлы [103, 94-95].

В силу изложенного такая технологически возможная деятельность, по существу, превращается в самостоятельный способ обнаружения, закрепления и изъятия следов преступлений в компьютерных сетях. Однако к настоящему времени ее правовое регулирование в законодательстве отсутствует, в связи с чем, она применяется лишь в качестве одной из составляющих отслеживания сообщений, передаваемых по сетям электросвязи, и реализуется в правовом режиме оперативно-розыскных мероприятий при их проведении в реальном масштабе времени.

Однако, как известно, розыск традиционно трактуется как «разрабатываемая криминалистикой система следственных, розыскных и оперативно-розыскных мероприятий, направленных на установление и задержание преступника, обнаружение и изъятие похищенного имущества, оружия и орудий преступления, а также иных объектов, имеющих значение для расследования и разрешения дела по существу» [101, 9].

Следует отметить, что пределы розыска обычно ограничены физическими или логическими границами конкретного места или территории его проведения. Однако компьютерная сеть может размещаться и не в одном месте, а быть соединена с другими частями сети посредством постоянных или периодически включаемых линий связи. Естественным в таких случаях является вопрос о том, допустимо ли проводить розыск в соединенных системах, если элементы таких систем расположены вне таких границ и требуется ли получение санкция прокурора при выявлении новых элементов компьютерной сети при возможном проведении такого розыска? Вопрос еще более осложняется, если удаленный терминал, с которого или на который осуществлялся выход в ходе розыска, расположен на значительном удалении (например, в другом городе).

Учитывая уже отмечавшиеся особенности компьютерной информации, легкость ее уничтожения и изменения, такая постановка вопроса является от-

нюдь не риторической. С точки зрения норм закона — да, требуется новое процессуальное решение. Но в то же время это может означать, что за то время, пока оно будет вынесено, доставлено к месту нахождения удаленного терминала или компьютера, разыскиваемая требуемая конкретная компьютерная информация может быть уничтожена. «В крупных сетях физическое местонахождение компьютерных данных и их носителей (например, конкретного физического сервера) может быть вообще не установлено, или он будет недоступен физически, с сохранением лишь виртуального доступа по компьютерным сетям» [104, 44]. В подобных случаях обращение за санкцией в прокуратуру крайне проблематично, поскольку отсутствуют координаты возможного местонахождения компьютерной информации.

С учетом того, что собирание доказательств по уголовному делу возложено на лицо, производящее дознание, следователя, то перечисленные лица должны быть законодательно наделены полномочиями по розыску в компьютерных сетях (или в среде для хранения компьютерных данных) с целью обнаружения и изъятия искомой компьютерной информации, которая после надлежащего документирования может стать доказательством.

Вопрос о наделении органа уголовного преследования такими полномочиями и разработка механизма действия данного положения является самостоятельной научной проблемой и требует более детального анализа. В качестве примера можно привести историю возникновения и реализации программы СОРМ (специальные оперативно-розыскные мероприятия), введенной в Российской Федерации. На ее разработку и внедрение ушло несколько лет и до сих пор ведутся дискуссии о ее правомерности отлаженности действия.

В настоящее время решением проблемы обнаружения и получения информации в компьютерных сетях является перехват сообщений, который по существу производства является разновидностью обыска — обыска в компьютерных сетях (или в среде для хранения компьютерных данных) с целью изъятия искомой компьютерной информации. В отличие от упомянутого ранее розыска в компьютерных сетях, когда местонахождение информации неизвестно, такой обыск должен проводиться при условии, когда примерное место ее нахождения известно. Именно это должно определять регулирование правового режима перехвата сообщений.

Означенные выше проблемы и назревающая необходимость использования действующего законодательства для решения вопросов, связанных с получением и закреплением информации с технических каналов связи и компьютерных систем, нашла частичное разрешение в производстве такого следственного действия как осмотр. Его цель — с помощью специалиста установить, зафиксировать и изъять следы совершенного преступления, которые в дальнейшем, в процессе расследования уголовного дела, могут быть признаны в качестве вещественных и иных доказательств, а также получить иную необходимую информацию при осуществлении перехвата сообщений.

При проведении осмотра, связанного с противоправным использованием компьютерных сетей, следует иметь в виду следующие обстоятельства.

Во-первых, учитывая особенности компьютерной информации, необходимо обеспечить ее обязательное документирование.

Во-вторых, осмотр, проводимый до возбуждения уголовного дела, является единственным процессуальным действием, проводимым в целях обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а равно иных обстоятельств, имеющих значение для дела.

В-третьих, при осмотре места происшествия, связанным с совершением преступлений в компьютерных сетях, учитывая необходимость обнаружения и закрепления специфических следов, приглашение специалиста является обязательным.

Необходимость обязательного участия специалиста связана не только с особенностями обнаружения, но и с проблемой фиксации следов в виде компьютерной информации. Закрепление и изъятие следов компьютерных преступлений как в процессуальных режимах осмотра, выемки или обыска в соответствии с действующим УПК, так и в ходе ОРМ фактически не обеспечивают их сохранности в том виде, в каком они обнаружены. Это обусловлено тем, что «виртуальные следы» в силу их особенностей не могут быть изъяты. Может быть проведено лишь их копирование с использованием различных программно-технических средств (использование которых и требует специальных познаний, навыков), в ходе которого обязательно изменяются отражаемые в файле дата и время последней операции, которые замещаются датой и временем самого копирования. Это влечет за собой потерю существенно важной в доказывании по таким делам информации о фактических дате и времени создания копируемого файла. Однако действующее уголовно-процессуальное законодательство, регламентируя порядок привлечения специалистов к участию в следственных действиях, не учитывает отмеченных особенностей следов в сфере компьютерной информации, не регламентирует особый (с применением программно-аппаратных средств) порядок их фиксации (копирования), не определяет особых условий этого, что существенно затрудняет признание доказательствами откопированной компьютерной информации.

При расследовании преступлений одним из самых важных и первостепенных следственных действий является осмотр, с помощью которого следователю приходится извлекать значимую информацию из определенного участка местности, помещения, различных предметов и вещей, электронно-вычислительной техники (ЭВТ).

Порядок осмотра подробно раскрыт в процессуальной и криминалистической литературе, и следователь всегда руководствуется общими правилами осмотра. При этом следователь обращает особое внимание на условия обнаружения вещественного доказательства, которые должны быть точно и детально указаны в протоколе. Это имеет важное значение для оценки вещественного доказательства, определения, в частности, его относимости. В связи с чем, возникает необходимость подробно описать место обнаружения и изъятия вещественного доказательства. Как правильно заметил В. Д. Арсеньев: «место обна-

ружения вещественных доказательств играет такую же роль для определения их доказательственного значения, как личность свидетеля или потерпевшего — для определения доказательственного значения их показаний» [105, 82]. При обнаружении, «вещественный объект необходимо тщательно осмотреть, выявив все те его свойства и признаки, которые могут иметь отношение к обстоятельствам, подлежащим доказыванию. Все это должно быть описано в протоколе осмотра вещественного доказательства, с обеспечением полноты и точности сведений о свойствах и признаках предмета, имеющих доказательственное значение» [106, 240].

Но за последнее время появился ряд предметов и вещей, осмотр которых если не затруднен, то, по крайней мере, достаточно сложен, а необходимой методической литературы почти нет. Речь идет об электронно-вычислительной технике, использование которой имеет много преимуществ по сравнению с обычной записной книжкой и объем информации, находящийся в ней достаточно велик.

Компьютер, как объект процессуальных действий, нередко попадает в сферу деятельности правоохранительных органов. Он может являться орудием совершения преступления (неправомерный доступ к информации, ее уничтожение и другое), похищенным имуществом, базой данных хранения различных видов информации (личной, служебной и тому подобной), средством передачи и получения сообщений и другого. В связи с чем, возникает необходимость рассмотрения особенностей производства осмотра компьютера, производимого с целью обнаружения и изъятия информации, интересующей следствие из памяти ЭВМ, или ее периферийных устройств.

При получении информации с технических каналов связи, снятии ее с компьютерных систем, а также при производстве обыска (выемки), осмотр компьютера может проводиться с целью идентификации компьютера, на котором формировалось (или с которого было отправлено) отдельное сообщение или установления признаков как похищенного имущества. Производство обыска с осуществлением осмотра компьютера будет носить комбинированный характер. Во многих случаях это просто необходимо. Как справедливо указал В. В. Крылов: «обыск, выемку и осмотр при расследовании компьютерных преступлений (и производстве отдельных следственных действий — примечание А. С.) целесообразно производить в форме “обысков-осмотров”» [65, 74]. Подтверждением данного высказывания является протокол обыска по уголовному делу № 420081201. При изучении данного документа и уголовного дела в целом установлено, что в связи с тем, что следователь при производстве обыска в квартире подозреваемого К. обнаружил в одной из комнат компьютер, не изымая компьютер для дальнейшего исследования, он путем производства осмотра исследовал текстовые файлы, находящиеся в ЭВМ и обнаружил информацию, которая в последующем помогла установить соучастников преступления и являлась доказательством виновности К. в совершенном преступлении. Отметим, что если бы следователь произвел исследование компьютера хотя бы на сутки

позже, то задержать соучастников было бы гораздо сложнее, так как последние были задержаны на вокзале, собираясь уехать за границу [107].

Фактически оптимальный вариант организации и проведения осмотра ЭВМ и машинных носителей информации — это фиксация их и их конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или по месту производства следствия с участием специалистов. Следователю необходимо соблюдать отдельные тактические приемы, которые позволят недопустить утрату доказательственной информации. Перечень приемов определен методическими рекомендациями по расследования преступлений в сфере компьютерной информации [108, 16], а также казахстанскими [109, 268; 110, 15] и российским [111, 210] учеными. На основе анализа указанных источников, обобщения рекомендуемых приемов предлагается: «По прибытии на место непосредственного действия необходимо:

- быстро и неожиданно войти в помещение, чтобы свести к минимуму возможность уничтожения информации, находящейся на компьютере. В некоторых случаях, когда это возможно и целесообразно, непосредственно перед входом в обыскиваемое помещение следует обесточить его;
- не разрешать, кому бы то ни было из лиц, работающих на объекте обыска, или иным лицам, прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры, при необходимости удалить персонал в другое помещение;
- если перед началом обыска электроснабжение было отключено, то до его подключения следует отключить от электросети все компьютеры и периферийные устройства;
- не разрешать, кому бы то ни было из персонала выключать или включать электроснабжение объекта;
- 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 стиранию информационных ресурсов на данном компьютере);
- 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;

- не производить никаких манипуляций с компьютерной техникой, если их результат заранее неизвестен;
- 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.

После выполнения вышеуказанных рекомендаций следует произвести внешний осмотр средств ЭВМ с подробным описанием всего наблюдаемого в протоколе. Главным является грамотное и правильное описание в протоколе состояние наблюдаемого ЭВМ и ее аппаратных устройств во взаимосвязи между собой, описание процесса разъединения средств ЭВМ друг от друга, описание опечатывания разъемов возникших после разъединения соединительных электрических проводников, описание опечатывания дисководов, обследование на предмет обнаружения отпечатков следов пальцев рук на клавиатуре, правильная упаковка изъятых объектов». Для более качественного установления вышеозначенных аспектов можно воспользоваться помощью специалиста в области компьютерных технологий.

В ходе поиска и изъятия информации и следов воздействия на нее вне ЭВМ могут быть обнаружены имеющие значение вещественных доказательств:

а) документы, носящие следы совершенного преступления, — телефонные счета, пароли и коды доступа, дневники связи и прочие;
б) документы со следами действия аппаратуры. Например, в устройствах вывода (например, в принтерах) могут находиться бумажные носители информации, которые остались внутри в результате сбоя в работе устройства;
в) документы, описывающие аппаратуру и программное обеспечение;
г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что преступник их знал и умышленно нарушал;
д) личные документы подозреваемого или обвиняемого.

Прежде всего, рекомендуется не забывать при осмотрах электронно-вычислительной техники о возможностях сбора традиционных доказательств (отпечатков пальцев рук на клавиатуре, выключателях и других, шифрованных рукописных записей и прочем).

При осмотре, проводимом в каком-либо учреждении, должен присутствовать кто-либо из сотрудников, 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 осуществить «взлом» паролей и кодов, осуществить надлежащий осмотр компьютера и содержащихся на нем файлов. В таких случаях достаточно изъять только системный блок, в который входят жесткий диск, процессор, накопители на магнитных дисках.

Остальную часть компьютера — монитор, клавиатуру, принтер — следует опечатать.

Если непосредственный доступ к информации на компьютере возможен и все нежелательные ситуации исключены, при осмотре следователь и специалист должны четко объяснять понятым все совершаемые ими действия.

При производстве осмотра компьютера, следователю, в первую очередь, необходимо:

- отразить в протоколе точное местонахождение компьютера и его периферийных устройств (принтера, модема, клавиатуры, монитора, джойстика, мыши, светового пера, микрофона, факс-модема, стримера, сканера, плоттера и других);
- определить и указать в протоколе тип, модель и иные характеристики электронных устройств, входящих в состав ЭВМ; назначение каждого устройства, название (обычно указывается на лицевой стороне), номер модели и серийные номера каждого из устройств, инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия; комплектацию (наличие и тип дисководов, сетевых карт, разъемов и так далее), наличие соединения с локальной вычислительной сетью и (или) сетями телекоммуникации, состояние устройств (целое или со следами вскрытия); прочую информацию с фабричных ярлыков;
- с помощью специалиста установить наличие внутри компьютера нештатной аппаратуры, а также внутренних накопителей и устройств для работы с другими машинными носителями (дискеты, компакт-диски, магнитооптические диски и другие);
- точно описать порядок соединения между собой указанных устройств, промаркировав (при необходимости) соединительные кабели и порты их подключения.

При наличии отключенных внешних периферийных устройств (модем, сканер, принтер и других) указать на возможность их подключения. Проверить их работу с исследуемым компьютером (при возникновении такой необходимости) можно в ходе следственного эксперимента [112, 51]. Например, в ходе производства обыска по уголовному делу № 980710 по факту фальшивомонетничества, где в одной из комнат был обнаружен компьютер, в других — сканер и цветной принтер. Здесь же следователем было принято решение о производстве следственного эксперимента. При подсоединении данных устройств было установлено, что исследуемые периферийные устройства имели программное обеспечение, установленное в данном компьютере, и, как затем было установлено, именно с их помощью преступники изготавливали поддельные купюры [69].

Если в ходе осмотра компьютера, будь то в процессе обыска или производства осмотра, возникает необходимость включения компьютера, его запуск следует осуществлять с заранее подготовленной загрузочной дискеты, исключив тем самым запуск программ пользователя. После чего, следователь, с учетом

обстоятельств дела, складывающейся следственной ситуации и степени его подготовленности к проведению рассматриваемых следственных действий, может приступить ко второй стадии — обследование внутрикорпусного содержания ЭВМ, для поиска интересующей следствие информации.

Суть этих действий состоит в поиске информации в памяти ЭВМ и ее аппаратных средствах, с целью ее изъятия, осмотра и приобщения к материалам дела. Сама процедура должна происходить с обязательным участием специалиста в области компьютерной техники, поскольку уменьшается риск уничтожения следователем искомой информации по незнанию, неосторожности и другим причинам. В качестве специалистов могут выступать сотрудники оперативно-технических подразделений. При выполнении указанных действий необходимо соблюдать следующие правила.

Определить, какая программа выполняется в данный момент. Для этого изучается изображение на экране дисплея и детально описывается в протоколе. При необходимости осуществляется фотографирование или видеозапись изображения на экране дисплея. После остановки программы и выхода в операционную систему иногда при нажатии функциональной клавиши «F3» можно восстановить наименование вызывавшейся последний раз программы.

Остановить исполнение программы и зафиксировать в протоколе результаты своих действий, отразить изменения, произошедшие на компьютере. Остановка многих программ осуществляется одновременным нажатием «Ctrl-C», либо «Ctrl-Break», либо «Ctrl-Q». Часто для окончания работы с программами следует ввести с клавиатуры команды «EXIT» или «QUIT», иногда достаточно нажать клавишу «Esc» или указать курсором на значок прекращения работы программы. Результаты своих действий, произошедших изменения, следует отразить в протоколе.

Определить наличие у компьютера внешних устройств — накопителей информации на жестких магнитных дисках (винчестере), на дискетах и устройствах типа ZIP, наличие виртуального диска (временный диск, который создается при запуске компьютера для ускорения работы), отразив полученные данные в протоколе.

Определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (подключение к локальной сети, наличие модема), отразить в протоколе результаты своих действий, после чего соединить сетевые кабели так чтобы никто не мог изменить или стереть информацию.

Скопировать интересующие файлы данных, созданные на виртуальном диске (если он имеется), на магнитный носитель или на жесткий диск компьютера в отдельную директорию. Копирование осуществляется стандартными средствами ЭВМ. Если возникает необходимость (и возможность), следователь может изъять информацию с ЭВМ, путем копирования ее на магнитный носитель и удаления с винчестера компьютера. В дальнейшем, если изъятая информация не представляет интереса для следствия, она возвращается владельцу под расписку.

При осуществлении осмотра компьютерной техники следует обращать внимание не только на физические носители информации (винчестеры и содержащиеся в них файлы), но и на оперативные запоминающие устройства (ОЗУ) ЭВМ, которые также могут нести в себе интересующую следствие информацию. Существуют следующие виды ОЗУ.

1. *Оперативное запоминающее устройство (ОЗУ) ЭВМ.* При запуске компьютера в ОЗУ ЭВМ загружаются в определенном порядке файлы с командами (программами) и данными, обеспечивающими для ЭВМ возможность их обработки. Последовательность и характер такой обработки задается сначала командами операционной системы, а затем командами пользователя. Сведения о том, где и какая информация хранится или какими командами обрабатывается в ОЗУ, в каждый конкретный момент времени доступны пользователю и при необходимости могут быть им получены немедленно с помощью стандартных инструментов, существующих, например, в системе Windows-2000.
2. *ОЗУ периферийных устройств.* В процессе обработки информации ЭВМ ведет активный обмен информацией со своими периферийными устройствами, в том числе с устройствами ввода и вывода информации, которые, в свою очередь, нередко имеют собственные ОЗУ, где временно хранятся массивы информации, предназначенные для обработки этими устройствами. Примером такого устройства является, в частности, лазерный принтер, где могут стоять «в очереди на печать» несколько документов. Устройство ОЗУ периферийных устройств сходно с ОЗУ ЭВМ. Оно поддается контролю и управлению и, следовательно, является носителем компьютерной информации.
3. *ОЗУ компьютерных устройств связи и сетевые устройства.* Большинство периферийных устройств связи (модемы и факс-модемы) имеют свои ОЗУ или «буферные» устройства, где находится информация, предназначенная для дальнейшей передачи. Время нахождения в них информации может быть различным и исчисляться от секунд до часов.

При поиске и изъятии информации и следов воздействия на нее в ЭВМ и ее устройствах следует исходить из того, что в компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на дисплее. Однако следует учитывать, что если возникла необходимость изъятия информации из оперативной памяти компьютера (непосредственно из оперативного запоминающего устройства — ОЗУ), то сделать это возможно только путем копирования соответствующей машинной информации на физический носитель с использованием стандартных паспортизированных программных средств, с соответствующим документальным приложением.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ. Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

При отсутствии специалиста интересный выход из данной ситуации был найден одним из следователей. Запросив необходимые сведения, он получил от специалистов рекомендации в письменном виде, согласно которым нужно сделать следующее: «… при включении компьютера на экране выдается таблица программной оболочки “Norton Commanders”, жесткий диск может быть разделен на части, поэтому нажмите одновременно две клавиши “Alt +FI” — на экране появится картинка с именами всех дисков, которыми оперирует данный компьютер. Если у компьютера два дисковода, что видно из наружного осмотра, то им соответствуют латинские буквы “A” и “B” (если дисковод один, буква “B” отсутствует). Буквы, начиная с “C”, соответствуют разделению жесткого диска на части. При наличии устройства для чтения лазерных дисков ему соответствует последняя в списке буква (при одном дисководе ему может соответствовать и буква “B”). Выделите курсором букву “C”, нажмите клавишу “Enter” и в левом окне появится список программ, записанных на диске “C”.

В списке будут записи двух видов — файлы, написанные строчными буквами (это могут быть отдельные программы или служебные файлы), и каталоги, написанные прописными буквами. Если курсор установить на название каталога и нажать клавишу “Enter”, то на экране появится список файлов, входящих в данный каталог. Каталоги имеют иерархическую структуру и могут быть вложены один в другой. Все их необходимо переписать. Каждая программа занимает определенный объем на диске. Размер программы указан в нижней строке, ограниченной двойной рамкой. Для того чтобы определить размер целого каталога, после входа в него следует нажать клавишу “большой серый плюс” на цифровой клавиатуре и клавишу “Enter”. Каталог (все входящие в него программы) будет выделен другим цветом, а в нижней строке будет указан его объем. При наличии принтера эту информацию необходимо распечатать, в противном случае — переписать от руки.

Когда в левом окне будет находиться оглавление диска “C”, его же необходимо вывести в правом окне (для этого нажать одновременно клавиши “Alt+F2”). После этого следует вывести в окно содержимое первого по списку каталога, включить принтер, заправить в него бумагу, а на клавиатуре ЭВМ нажать клавишу “Print Screen”, после чего на бумаге появится точная копия экрана монитора. Данную операцию следует повторить для всех каталогов диска “C”, каждый раз выдавая картинку на печать (одновременно возможно выдавать два каталога, вызвав их в правом и левом окнах). Аналогичным образом должны быть сделаны распечатки всего жесткого диска (“D”, “E” и так далее)» [113]. Используя данные рекомендации, следователь успешно провел исследование и получил необходимые сведения.

В тех же случаях, когда исследование проводится с участием специалиста, все листы с информацией должны быть подписаны специалистом, который проводил запись информации, следователем, понятыми и представителем организации (пользователем), где производится осмотр, и прилагаться к протоколу следственного действия.

Для копирования информации в ходе осмотра необходимо иметь:

- предварительно отформатированные дискеты;
- коробки (желательно пластиковые) для хранения дискет;
- пакеты для упаковки дискет в коробке;
- материал для опечатывания дискет и компьютеров.

Поиск и осмотр информации, находящейся в компьютере, включает в себя проблему исследования большого объема данных, расположенных на машинном носителе. И ее прочтение может занять довольно таки продолжительное время, а ее фиксация — еще больше. Как же здесь быть? Ответ может быть такой: может читаться и фиксироваться только искомая информация (например: телефон, адрес, определенный текст). Для уменьшения времени чтения данных, возможно применение различных программ, облегчающих поиск и просмотр информации, ее раскручивание и обзор свойств отдельных файлов. При осмотре информации обязательно нужно указывать последовательность проводимых операций и в наименования раздела, где эта информация была считана.

Необходимо произвести детальный осмотр файлов и структур их расположения; лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя. Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Осмотр физических носителей магнитной информации (например, дискет), как правило, особых трудностей не представляет, но и его необходимо проводить с участием специалиста. Если информация на них не имеет значения для следствия, то такие дискеты подлежат возврату по принадлежности. Если же у специалиста имеются хотя бы малейшие подозрения относительно информации, находящейся на дискетах, они должны быть скопированы, опечатаны и изъяты для проведения тщательной экспертизы.

При копировании информации с дискет необходимо повторить все те же операции, которые были описаны для работы с жестким диском. Причем их следует произвести с каждой осматриваемой дискетой отдельно. Для этого дискеты поочередно вставляют в дисковод ПЭВМ и аналогичным образом распечатывают их содержимое.

Перед тем как закончить работу с дискетой, целесообразно снять с нее две копии: одна оставляется в качестве контрольного экземпляра; вторая предназначается для проведения экспертизы.

Завершив работу с дискетой, следует:

- на дискете 3,5 дюйма открыть окно слева, опечатать его;

– на дискете 5,25 дюйма опечатать вырез в верхней части правой стороны.

Эта операция обеспечит защиту записи на данной дискете.

Все документы, полученные в результате работы с дискетами, должны быть подписаны, упакованы в коробки и опечатаны согласно процедуре.

Весь процесс и результаты следственного действия должны быть тщательно зафиксированы в протоколе.

При этом в описательной части протокола необходимо отразить все действия, производимые следователем, обстановку, местонахождение и состояние предметов и документов. Следует охарактеризовать и индивидуализировать компьютер (или его составную часть), указать номер, марку, форму, цвет, размер и прочее, чтобы можно было отличить от сходных предметов. Особо выделяются изменяющиеся признаки и особенности, которые со временем могут быть утрачены (влажность, напыление, помарки и так далее).

В качестве примера описательной части протокола осмотра компьютера приведем выдержку из материалов уголовного дела № 1750200:

«Осмотром установлено:

Компьютер находится в помещении ... по адресу: ...

Комплект компьютера состоит из 4 устройств:

1) системного блока, 2) монитора, 3) клавиатуры, 4) манипулятора — мышь.

1. Системный блок модели “ST-406 LT PASS HIPOT PASS FDD PASS Sl”. Фирмы “KRAFT COMPUTER”. На задней панели прозрачной липкой лентой наклеен на полоске бумаги номер — 1241708/4. Системный блок имеет 3 входа: 1 — с надписью “POWER”; 2 — без надписи; 3 — с надписью “KEYBOARD”. Все подключены.

Имеет 5 выходов: 1 — “corn 2”; 2 — “game”; 3 — “printer”; 4 — “mouse”; 5 — “svga”, из которых подключены выходы 4 и 5.

На лицевой панели два дисковода размером 3,5 и 5 дюймов, клавиши: включения, “Reset”, “turbo”, “lock”, окно частоты. На момент начала осмотра компьютер отключен.

2. Монитор фирмы “Daewoo”, модель CMC-14276. Серия № 5126E0019. Произведено в декабре 1995 г. в Корее. Инвентарный номер отсутствует. На момент начала осмотра монитор отключен.

3. Клавиатура — FCC1DE8HKB-2313. Модель № KB-2313. Серия 5K83002684. На нижней панели прозрачной липкой лентой наклеен на полоске бумаги номер — 01380432. К моменту начала осмотра — отключена.

4. Мышь FCCIDEMJMUSGC. На нижней панели имеется наклейка из белой бумаги с надписью “MUSC GL V 34A AA (T6)”. Мышь овальной формы размером 4,5×П см из пластмассы серого цвета, на верхней поверхности имеет 3 клавиши. К моменту начала осмотра отключена.

В ходе осмотра компьютер включен в штатном режиме. Перед загрузкой операционной системы сведения о защите компьютера паролем или иными средствами защиты не выявлены. После загрузки на экране появилась таблица

программы “Norton Commander (NC)”. Жесткий диск разделен на две части, обозначенные “C” и “D”.

На диске “C” находятся 12 каталогов (ARCH, AVIR, DOS, DRIVER, DRWEB, FOXPR025, INFIN.PLL, KEYRUS. LETTRIX, LEX, NC, TOOLS) и 12 программ (Image.idx, io.sys, Msdos.sys, autoexec.bak, autoexec.bat, command.com, config.sys, dwf.exe, image.dat, norton.ini, op.bat, printer.bat), занимающие 45978 байт памяти.

На диске “D” находятся 24 каталога (ARH, BUHGALT. CLIPPER5, DRV, INFIN, KARAT, N196, N296, N396, N496, N596, NAL, NAL1, NAL2, NAL3, NAL4, NAL5, PENS, PENSION, PLAT, SPR, VED, XTGOLD, ZARP) и 5 программ (Archbase.bat, dwf.exe, infin.com, infin.ins, infin.ovl), занимающие 29333 байт памяти).

Сведения об информации, находящейся на дисках “C” и “D”, распечатаны на принтере с помощью клавиши “Print Screen”. В распечатках указывается объем памяти, который занимает каждый каталог. Распечатки в полном объеме на ... листах прилагаются к настоящему протоколу.

После завершения распечатки все программы и информация, содержащиеся на дисках “C” и “D”, откопированы на 30 (15×2) дискетах “Verbatim”. Один комплект копий (15 дискет) передан специалисту Головач В. И., другой (15 дискет) упакован в две прозрачные пластмассовые коробки, которые опечатаны печатью ... №. ...

После завершения копирования компьютер выключен и отключен от сети, соединительные кабели извлечены из своих гнезд, входы и выходы системного блока опечатаны печатью №..., сам процессор упакован в картонную коробку, которая проклеена лентой-скотч, опечатан печатью ... № ...» [114].

Характеризуя компьютерную информацию, следует отметить, что она занимает на машинных носителях определенный ограниченный объем, который принято называть файлом. Ее типичные и факультативные свойства, выделяемые в специальной литературе [65, 235; 115, 300; 116, 22], на наш взгляд, с криминалистической точки зрения, могут быть использованы для идентификации файла и находящейся в нем информации, что имеет важное значение при расследовании компьютерных преступлений.

Так, файлы как физические объемы, находящиеся на различных машинных носителях информации, имеют общие типичные свойства:

1. Наименование файла (включая его местоположение на логическом диске — «путь»).
2. Размер файла.
3. Время создания, модификации.
4. Системные атрибуты («системный», «только для чтения» и другие).
5. Тип информации, хранящейся в файле (текстовая, графическая и так далее).
6. Машинный носитель, его тип, номер, метка и другое.

Кроме типовых свойств файлы могут обладать и иными свойствами, позволяющими их характеризовать, иногда их называют факультативными свойствами:

1. Программные средства, с использованием которых был создан или модифицирован файл (использование специальных символов, выделений, отметок в коде программы или документе, указателей на версию, серийный номер программного продукта, зарегистрированный пользователь программного продукта и другое).
2. Автор, создавший или модифицирующий файл (программу в целом).
3. Группа файлов (программные средства, группы документов), куда включен файл (в качестве отдельного документа или части программного кода).
4. Ключевые слова, заметки автора или редактора и тому подобное.

Приведенные выше свойства файлов, при отражении их в протоколах следственных действий, позволят удостоверить относимость, допустимость и достоверность полученной информации, при ее дальнейшем использовании в качестве доказательств при расследовании уголовных дел. В качестве примера изложения основных параметров исследуемого компьютера и входящей в него информации, приведем выдержку из протокола осмотра ЭВМ по уголовному делу, возбужденному по факту фальшивомонетничества с использованием персонального компьютера.

«… Осмотрен компьютер IBM на базе процессора P-133, стоящий из: монитора “Gold Star”, модель “1460 SVGA”, клавиатуры “Beltron”, системного блока — P-133, 16, 16 Мв RAM, 426 Mb HDD/жесткий диск, CD-ROM-2x, FDD — 5, 25, 35 trident, SVGA 512 Kb, sound ESSES 688. При включении, на мониторе появляется файловая оболочка “DOS”, через нажатие “Alt+x”, загружается “Win-95, запускается программа “Adobe” с помощью которой …

Файл, в котором содержится изображение денежных купюр, лежит в каталоге c:\Mscan\Msoffice\temp с именем p1941690$. При просмотре данного файла на мониторе появляется изображение денежной купюры, достоинством 200 тенге. … В операционной системе “Win-95” установлен драйвер для принтера “Epson Stylus 440”» [69].

Осуществляя получение информации с технических каналов связи и компьютерных систем, орган, технически осуществляющий перехват сообщений, постоянно информирует следователя о результатах и в случае получения интересующей информации незамедлительно сообщает о ней. В случае передачи перехваченных сообщений следователю, орган, осуществляющий данное следственное действие, направляет материал с официальным сопроводительным письмом, в котором указываются основания перехвата, время начала и окончания данных действий, суть информации и количество страниц. Копия дискеты передается следователю в опечатанном виде

Для опечатывания дискет необходимо:

– упаковать их в жесткую коробку, опечатать ее;

- на листе бумаги сделать описание упакованных дискет: количество, тип каждой из них, что указано на бирках (если они есть);
- коробку с дискетами и лист с описанием положить в полиэтиленовый пакет, который заклеить.

При опечатывании дискет недопустимо производить какие-либо действия с самими дискетами. Аналогично следует опечатать копии, снятые на месте.

При необходимости изъятия магнитных носителей, компьютера и (или) периферийных устройств, следователю следует их опечатать.

При опечатывании компьютеров не следует пользоваться жидким клеем или другими веществами, которые могут испортить его. Наиболее просто рекомендуется опечатывать компьютер в следующей последовательности:

- выключить компьютер;
- отключить его от сети;
- отсоединить все разъемы, опечатав каждый из них;
- на длинную полосу бумаги следует поставить подписи следователя, специалиста, понятых, представителя персонала или администрации и номер. Эту полосу наложить на разъем и приклеить. В качестве клеящего средства использовать липкую ленту или густой клей. При использовании липкой ленты ее надо наносить так, чтобы любая попытка снять ее нарушала бы целостность бумажной ленты с подписями;
- аналогично должен быть опечатан разъем шины (соединительного провода). При этом номера на разъемах блока компьютера и шины должны быть одинаковыми. Для облегчения операции сборки и подключения компьютера в дальнейшем на бумажной полосе, опечатывающей шину, можно указать, к какому блоку должен подключаться разъем. Например: «I — системный блок». На другом конце той же шины может стоять надпись «2 — монитор»;
- если бумажная лента достаточно длинная, ее можно крепить к боковым поверхностям блоков компьютера либо к поверхности стенки, но так чтобы не задевать другие детали.

Для упаковки могут использоваться как специальные футляры, так и обычные бумажные и целлофановые пакеты, исключающие попадание грязи и тому подобного на рабочую поверхность дискеты или магнитной ленты.

Транспортировка и хранение компьютерной техники и физических носителей магнитной информации должны осуществляться с соблюдением следующих основных мер безопасности:

1) при перевозке компьютеров следует исключить их механические или химические повреждения;
2) не допускать магнитных воздействий, как на компьютеры, так и на магнитные носители информации, так как это может привести к порче или уничтожению информации путем размагничивания;

3) оградить изъятое от воздействия магнитосодержащих средств криминалистической техники (например: магнитных подъемников, магнитных кисточек для выявления следов рук и прочего);
4) соблюдать правила хранения и складирования технических средств;
5) нельзя ставить компьютеры в штабель выше трех штук, а также ставить их на какие-либо другие вещи;
6) помещение для хранения должно быть теплым, отапливаемым, без грызунов;
7) компьютеры нельзя держать в одном помещении со взрывчатыми, легко воспламеняющимися, огнеопасными, едкими, легко испаряющимися химическими препаратами, а также с предметами, которые могут создавать магнитные поля;
8) не рекомендуется курить, принимать пищу и содержать животных в помещениях, предназначенных для хранения компьютерной техники и магнитных носителей.

В то же время, следует отметить, что если пользование ЭВМ не вызывает больших трудностей, то считывание информации с паролем и без пароля имеет свои особенности. В случае если ЭВМ или интересующая следствие информация имеет пароль, необходимо назначить экспертизу, так как для прочтения информации требуются специальные познания в области программирования. Осмотр компьютера в данном варианте будет только внешний, то есть следователь обязан только идентифицировать ЭВМ для дальнейшего экспериментального извлечения искомой информации. Стоит отметить, что снятие пароля довольно таки сложная операция, которую можно поручить только техникам фирмы-представителя либо специалистам информационно-аналитических центров (как частного характера так и государственного). Особенности назначения данного вида экспертизы будут рассмотрены нами далее. Стоит отметить, что «в ряде случаев, технически это делается следующим образом: фирма изготовитель снимает материнскую плату с ЭВМ, и она вставляется в базовый компьютер, который и производит операцию снятия пароля и прочтение информации» [117, 41].

Конечно же, на практике производство такой экспертизы чрезвычайно сложно как в организационном плане, так и в финансовом. Но окружающий мир чрезвычайно быстро совершенствуется, появляются новые системы для сохранения и передачи информации, поэтому необходимо уметь пользоваться ими и правильно извлекать сведения для расследования преступлений (см. Приложение Д).

В связи с тем, что результаты исследования компьютерной экспертизы зависят от сохранности информации на внутренних и внешних магнитных носителях, необходимо при изъятии объектов и подготовке материалов на экспертизу соблюдать ряд правил:

- при проведении следственных действий необходимо исключить намеренную порчу или уничтожение хранящейся в компьютере информации;

- включать и выключать компьютеры, производить с ними различные манипуляции разрешать только соответствующему специалисту;
- при проведении следственных действий по изъятию компьютерной техники, а также других компьютерных частей к ним, необходимо участие специалиста, так как для сокрытия информации могут быть установлены специальные защитные программы, которые при определенных условиях автоматически производят полное или частичное уничтожение (стирание) информации;
- изъятые компьютеры и их комплектующие опечатываются путем наклеивания специальной ленты для исключения возможной работы с ними в отсутствие специалиста или эксперта;
- магнитные носители упаковываются, хранятся и перевозятся в специальных экранированных контейнерах или в стандартных пакетах либо иных футлярах заводского изготовления, исключающих разрушительное воздействие электромагнитных и магнитных полей и наводок направленных излучений;
- пояснительные надписи делаются на специальной самоклеящейся ленте (этикетка), опечатываются только контейнеры или футляры;
- категорически запрещается приклеивать непосредственно что-либо к магнитным носителям, делать отверстия, наносить подписи, наклейки, приставлять оттиски печати, штампов и так далее;
- перевозка и хранение компьютерной техники должны осуществляться в условиях, исключающих ее повреждение, в том числе результатов воздействия металлодетекторов, используемых для проверки багажа в аэропортах и железнодорожных станциях;
- хранить изъятые компьютеры необходимо в сухом, отапливаемом помещении, не ставя на них какие-либо другие предметы.

При получении перехваченных сообщений, следователю необходимо произвести осмотр полученной информации, в связи с чем, им приглашаются понятые, которые согласно ст. 86 УПК РК, являются лицами, привлеченными органом уголовного преследования для удостоверения факта производства следственного действия, его хода и результатов в случаях предусмотренных уголовно-процессуальным законодательством. Понятыми могут быть только незаинтересованные в деле и независимые от органов уголовного преследования совершеннолетние граждане, способные полно и правильно воспринимать происходящее в их присутствии действия.

Перехват сообщений является одним из процессуальных действий, в ходе которого становится известной информация о частной жизни лица. Участие понятых в производстве данного действия может поставить под угрозу распространение сведений, имеющих отношение исключительно к частной жизни лица. В связи с чем, сотрудники полиции, осуществляющие операции над получаемой информацией (в том числе и личного характера) должны руководствоваться в своей деятельности принципами уважения и защиты человеческого достоинства по отношению ко всем лицам. Данное требование было закреплено в

ст. 2 «Кодекса поведения должностных лиц по поддержанию правопорядка», принятого Генеральной Ассамблеей ООН и, кроме того, в ст. 4 установлено, что «Сведения конфиденциального характера, получаемые должностными лицами по поддержанию правопорядка, сохраняются в тайне, если исполнение обязанностей или требования правосудия не требуют иного. По характеру своих обязанностей должностные лица по поддержанию правопорядка получают информацию, которая может относится к личной жизни других лиц или потенциально повредить интересам таких лиц и особенно их репутации. Следует проявлять большую осторожность при сохранении и использовании такой информации, которая разглашается только при исполнении обязанностей или в целях правосудия. Любое разглашение такой информации в других целях является полностью неправомерным» [118, 308]. Принцип сохранения конфиденциальности закреплен в ст. 53 УПК Республики Казахстан. В целях обеспечения данного принципа закон также предусматривает возможность оглашения материалов, содержащих сведения частного характера, в закрытом судебном заседании, открытое их оглашение возможно лишь с согласия лиц, имеющих отношение к подобной информации.

В подобных ситуациях лицо, уполномоченное осуществлять расследование, обязано, наряду с правами участвующих, в порядке ст. ст. 53, 205 УПК РК, предупредить понятых и иных участников (при их присутствии) проводимого действия о недопустимости разглашения ставших им известными сведений и ответственности за их разглашение без согласия следователя по ст. 355 УК РК.

После разъяснения вышеозначенных положений следователь производит осмотр полученного машинного носителя, проверяет его подлинность, целостность, правильность оформления и хранения. Протокол осмотра составляется с соблюдением всех требований закона и должен содержать данные, характеризующие параметры носителя и его внешний вид, индивидуальные особенности, признаки возможного внесения изменений, содержание просматриваемой информации.

По окончании осмотра следователь в присутствии понятых упаковывает машинный носитель информации, опечатывает его своей печатью и скрепляет своей и понятых подписями. После чего ознакамливает участников следственного действия с содержанием протокола и в случае внесения замечаний, дополнений, изменений они оговариваются и удостоверяются подписями этих лиц. Протокол подписывается следователем, понятыми и всеми иными лицами, участвовавшими в производстве осмотра.

Следователь, ознакомившись с содержанием информации, вправе:

- приобщить материал в качестве вещественного доказательства к уголовному делу, составив соответствующее постановление, в соответствии с ч. 2 ст. 223 УПК РК;
- не приобщать перехваченную информацию к уголовному делу, а использовать ее для принятия процессуальных или тактических решений. Перехваченная информация, не приобщенная к делу, сдается в архив или возвращается органу, проводящему перехват сообщений и снятие

информации, для ее хранения или уничтожения. Информация, не имеющая отношения к делу, уничтожается после вступления приговора в законную силу или прекращения уголовного дела.

После производства осмотра полученная при перехвате сообщений информация, по решению следователя, может быть направлена адресату, блокирована или уничтожена. Об исполнении принятого решения дается соответствующее указание органу, производящему перехват сообщений.

В качестве примера оформления протокола осмотра перехваченных сообщений предлагается использовать разработанный автором образец документа, опубликованный в Примерных образцах уголовно-процессуальных актов досудебного производства:

Протокол просмотра перехваченных сообщений

г. Энск. 1 марта 2002 года.

Начат: 14 час. 25 мин.

Окончен: 14 час. 55 мин.

Следователь СО ГОВД г. Энска лейтенант полиции Симонов Р.Н. в присутствии понятых:

1. Сизовой Тамары Ильинишны, 1970 года рождения, проживающей по адресу: г. Энск, ул, Лободы, д. 23, кв. 86, паспорт № 87856, выдан МВД РК 26.06.96 г.

2. Истомина Ивана Иосифовича, 1967 года рождения, проживающего по адресу: г. Энск, ул. С. Лазо, д. 65, кв. 97, паспорт № 90857, выдан МВД РК 22.04.97 г. с соблюдением требований ст. ст. 203, 221, 222, 236 УПК РК, произвел просмотр информации, содержащейся на флоппи-диске «MFD-2HD» в кабинете № 44 СО ГОВД г. Энска, о чем составил настоящий протокол.

Перед началом осмотра перечисленным лицам разъяснено их право присутствовать при всех действиях, производимых в процессе действий производимых следователем, ознакомиться с протоколом, делать замечания подлежащие внесению в протокол.

Кроме того понятым Сизовой Т. И. и Истомину И. И. в соответствии со ст. 86 УПК РК разъяснена их обязанность удостоверить факт, содержание и результаты следственного действия, не разглашать без разрешения следователя материалы предварительного следствия, соблюдать порядок при производстве следственных действий, и они предупреждены об административной ответственности за отказ или уклонение от явки или от исполнения своих обязанностей.

Понятые: 1._____ Сизова Т. И. 2._____ Истомин И. И.

Кроме того, понятые, в соответствии со ст. 205 УПК РК, предупреждены об ответственности по ст. 355 УК РК за разглашение без согласия следователя сведений, которые стали им известны при производстве следственных действий.

Понятые: 1._____ Сизова Т. И. 2._____ Истомин И. И.

Объектом осмотра является:

Флоппи-диск «MFD-2HD», помещенная в целлофановый пакет, перевязанная бечевкой, концы которой скреплены сургучной печатью № 55 и биркой с надписью «Запись перехваченного сообщения с “электронного адреса: E-mail:rotari.rrrr.kaz Шапкин П.П.”».

Корпус кассеты из черного пластика, следов вскрытия не обнаружено. Для просмотра записи использовался компьютер «Pentium-155».

На флоппи-диске имеется один файл — «посылка.doc».

Содержание файла:

«Рерик, как у тебя делишки? Твой товар от последнего дела мы получили, продали за хорошую цену, жди своей доли с Толиком. Он приедет на этой неделе, привезет заказ и “стволы”. Встречай его на “малине” Гарика».

После просмотра данный флоппи-диск упакован в белый конверт, скреплен сургучной печатью № 11 и на нем сделана надпись «Запись перехваченного сообщения с “электронного адреса: E-mail:rota-ri.rrrr.kaz” 1 марта 1999 года». Конверт подписан понятыми и следователем.

Протокол зачитан следователем вслух, записано верно, замечаний и предложений не поступило.

Понятые: 1._____ Сизова Т. И. 2._____ Истомин И. И.

Следователь СО ГОВД г. Энска
лейтенант полиции _____ Симонов Р. Н. [95, 206].

Чтобы получить в свое распоряжение необходимую информацию (среди всего ее множества) о преступном использовании компьютерных сетей, следователь должен проследить цепочку коммуникаций (сеансов связи) от компьютера, в котором обнаружены следы преступления, до компьютера, на котором физически работало виновное лицо. При этом большинство таких сеансов связи осуществляется по сети «Internet», состоящей из множества локальных и глобальных сетей, принадлежащих различным компаниям и предприятиям, связанных между собой различными линиями связи. «Internet» можно представить себе в виде мозаики, сложенной из небольших сетей разной величины, которые активно взаимодействуют одно с другой, пересылая файлы, сообщения и тому подобное. В ходе сеанса связи информация проходит через значительное количество серверов, которые физически могут быть установлены не у меньшего количества провайдеров на значительном географическом пространстве и удалении. Тем не менее, даже при большом количестве «звеньев мозаики» возможно установление виновных лиц. Например, в Москве сотрудники ОВД вскрыли законспирированную сеть торговцев пиратскими CD-дисками, сбывавшими продукцию через интернет-магазин. Была отслежена цепочка курьеров, каждый из которых знал только следующее звено цепи. Сервер, через который делались заказы, был установлен в московской квартире, однако к «Internety» подключались через систему переадресации при помощи модемов и сотовых телефонов [119, 62].

Исходя из изложенного следует, что для того чтобы собрать достаточную совокупность доказательств виновности того или иного лица в преступлении,

совершенном с использованием возможностей глобальных компьютерных сетей, необходимо у каждого поставщика услуг (провайдера) получить в документированном виде сведения о сообщениях, передаваемых по сетям электросвязи (то есть те самые LOG-файлы).

Определенные в ходе исследования предложения диссертанта по особенностям формирования нормативной основы розыска в компьютерных сетях, были приняты во внимание законодателем при реализации положений, направленных на повышение эффективности борьбы с преступностью (см. Приложение Е) и нашли свое отражение в совместном Приказе Председателя Комитета национальной безопасности Республики Казахстан и и. о. Председателя Агентства Республики Казахстан по информатизации и связи «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», положениями которого определен порядок взаимодействия государственных органов и организаций при проведении оперативно-розыскных мероприятий на сетях телекоммуникаций. Согласно Правилам также определено, что операторы связи несут ответственность за сохранность установленных на объектах связи комплексов средств СОРМ и обеспечивают учет, регистрацию и хранение записей о произведенных пользователями соединениях, осуществляя запись на неперезаписываемый компакт-диск. Субъекты оперативно-розыскной деятельности вправе получать информацию об осуществленных соединениях для документирования фактов противоправной деятельности с соблюдением требований законодательства Республики Казахстан. Получение информации об осуществленных соединениях субъект оперативно-розыскной деятельности может получить путем направления провайдеру санкционированное прокурором постановления о снятии информации с технических каналов связи, компьютерных систем и иных технических средств [120].

Фактор времени часто имеет решающее значение при расследовании преступлений, и не случайно задачей уголовного судопроизводства ст. 8 УПК РК называет не только полное, но и быстрое раскрытие преступлений. Применительно к обнаружению следов преступлений, совершенных в сфере компьютерной информации, фактор своевременности установления и фиксации собранных доказательств имеет особое значение.

Это обусловлено тем, что «исторические данные» не только не всегда генерируются ЭВМ в объемах, достаточных в последующем для расследования преступлений, но многие из них в течение короткого времени уничтожаются. Для предотвращения их утраты, особенно в условиях, когда из иных источников становится предварительно известно о готовящемся преступлении, особое значение приобретает отслеживание сообщений, передаваемых по сетям электросвязи в реальном масштабе времени (основываясь на предполагаемых данных) с их фиксацией и установлением лица, осуществляющего незаконную деятельность, непосредственно во время совершения преступления.

Как известно, одним из основополагающих принципов отечественного уголовного процесса является всесторонность, полнота и объективность исследования обстоятельств дела. Сопоставление данного требования закона с особенностями следов в форме компьютерной информации свидетельствует, что именно отслеживание в реальном масштабе времени сообщений, передаваемых по сетям электросвязи, позволяет в наибольшей степени обеспечить полноту, всесторонность и объективность их обнаружения и закрепления.

Любому лицу довольно просто провести свое сообщение через множество компьютеров в «Internet», и лишь на последнем будет указан IP-адрес компьютера, с которого связывались напрямую, а не IP-адрес первоначального источника. Кроме того, «инфраструктура Internet обычно не имеет автоматического механизма идентификации источника. В силу этого в типичных случаях необходимо самим связываться с персоналом каждого оператора связи в транзитной цепочке сообщений для того, чтобы определить источник предыдущего сообщения. Если с этим персоналом оперативно связаться невозможно, то отслеживание вынужденно прекращается» [121, 75].

На основании проведенного выше анализа и исследования особенностей обнаружения и закрепления информации в технических каналах связи, в том числе компьютерных системах, сформулированы следующие выводы:

1. LOG-файлы являются специальными файлами регистрации. В них фиксируется техническая информация, содержатся данные о техническом обмене. В силу этого LOG-файлы (и соответственно сохраняемые ими сведения о сообщениях, передаваемых по сетям электросвязи) следует признать наиболее значимыми носителями следовой информации о совершении преступлений в компьютерных сетях и рассматривать как приложение к протоколу следственного действия или вещественное доказательство. Кроме LOG-файлов носителями доказательственной информации могут быть таблицы размещения файлов (FAT, NTFS или другие), системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное.

2. Изучение и анализ судебно-следственной практики Республики Казахстан, а также практики зарубежных стран, исследование их нормативной и теоретической базы позволяют обосновать необходимость разработки и введения в законодательство РК нормы, регламентирующей розыск в компьютерных сетях (или в среде для хранения компьютерных данных), проводимый с целью обнаружения и изъятия искомой компьютерной информации, которая после надлежащего документирования может стать доказательством при расследовании преступлений. Необходимо законодательно определить и наделить полномочиями по розыску в компьютерных сетях (или в среде для хранения компьютерных данных) специальные правоохранительные органы или службы. На основании изложенного предлагается при формировании правовых норм, регламентирующих розыск в компьютерных сетях (или в среде для хранения компьютерных данных), исходить из следующих положений:

а) розыск в компьютерных сетях (или в среде для хранения компьютерных данных) представляет собой систему процессуальных и оперативно-розыскных мероприятий, направленных на обнаружение, закрепление и изъятие в компьютерных сетях следов преступлений, а также иной компьютерной информации, имеющей значение для расследования и разрешения дела по существу;

б) телекоммуникационные службы и Internet-провайдеры обязаны по запросу правомочных правительственных учреждений и органов принять все необходимые меры к сохранению данных или других свидетельств, имеющихся в их распоряжении, до издания соответствующего решения, на основе которого эти данные изымаются в распоряжение органов правосудия;

в) компетентные органы вправе получить запрашиваемые данные в течение определяемого законодателем срока их хранения.

3. Компьютерная информация может иметь типичные и факультативные свойства, которые могут быть использованы для идентификации файла и находящейся в нем информации. Обозначенные свойства файлов, при отражении их в протоколах следственных действий, позволяют удостоверить относимость, допустимость и достоверность полученной информации, при ее дальнейшем использовании в качестве доказательства при расследовании уголовных дел.

4. Перехват сообщений является одним из действий, в ходе которого становится известной информация о частной жизни лица. В связи с чем, сотрудники полиции, осуществляющие операции над получаемой информацией (в том числе и личного характера), должны руководствоваться в своей деятельности принципами уважения и защиты человеческого достоинства по отношению ко всем лицам. Они обязаны в соответствии со ст. ст. 53, 205 УПК РК предупредить участников проводимого действия о недопустимости разглашения ставших им известными сведений и ответственности за их разглашение без согласия следователя по ст. 355 УК РК.

5. При проведении осмотра, связанного с противоправным использованием компьютерных сетей, учитывая особенности компьютерной информации, для ее исследования приглашать специалистов, участие которых позволит обнаружить и закрепить специфические следы электронной информации, устранит проблемы фиксации следов в виде компьютерной информации в процессуальных документах. В качестве примера оформления протокола осмотра перехваченных сообщений предлагается использовать разработанный автором образец документа.

6. В целях недопущения утраты доказательственной информации, необходимо соблюдать тактические приемы осмотра, исследования и изъятия компьютерной техники и информации.

Транспортировка и хранение компьютерной техники и физических носителей магнитной информации должны осуществляться с соблюдением основных мер безопасности, позволяющих недопустить их повреждение и утрату значимых сведений.

7. В случае если ЭВМ или интересующая следствие информация имеет пароль, необходимо назначить экспертизу, так как для прочтения информации из такой ЭВМ требуются специальные познания в области программирования. Снятие пароля довольно сложная операция, которую можно поручить только техникам фирмы-представителя либо специалистам информационно-аналитических центров.

8. Следователь, ознакомившись с содержанием информации, вправе:

а) приобщить материал в качестве вещественного доказательства к уголовному делу, составив соответствующее постановление, в соответствии с ч. 2 ст. 223 УПК РК;

б) не приобщать перехваченную информацию к уголовному делу, а использовать ее для принятия процессуальных или тактических решений.

Перехваченная информация, не приобщенная к делу, сдается в архив или возвращается органу, проводящему перехват сообщений и снятие информации, для ее хранения или уничтожения. Информация, не имеющая отношения к делу, уничтожается после вступления приговора в законную силу или прекращения уголовного дела.

9. Учитывая требования действующего законодательства и особенности прохождения информации в компьютерных сетях и остающихся при этом следов, в условиях временных ограничений, обусловленных краткостью периода хранения «исторических данных», решение задач по обнаружению, закреплению и изъятию органами дознания или предварительного следствия, следов преступлений в компьютерных сетях может достигаться:

а) путем обеспечения сохранности и изъятия в документированном виде ранее генерированных ЭВМ «исторических данных», в которых содержится информация о том или ином противозаконном деянии в компьютерной сети;

б) путем перехвата сведений о сообщениях, передаваемых по сетям электросвязи, в реальном масштабе времени.

Перехват на стадии передачи данных представляет собой операцию, целью которой является получение компьютерной информации, отсутствовавшей в момент ее начала. Изъятие в документированном виде «исторических данных» осуществляется в рамках процессуального действия, о производстве которого в установленном законом порядке информируются его участники.

Вместе с тем потребности, возникающие в ходе раскрытия и расследования преступлений, совершенных с использованием возможностей компьютерных сетей, не в полной мере могут быть удовлетворены лишь описанными способами собирания доказательств, что требует разработки и внесения соответствующих дополнений в уголовно-процессуальное законодательство.

3 ФОРМЫ ПРИВЛЕЧЕНИЯ СПЕЦИАЛЬНЫХ ПОЗНАНИЙ В ПРОЦЕССЕ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИИ С КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНИЧЕСКИХ КАНАЛОВ СВЯЗИ

3.1 Формы участия специалиста в сфере уголовного судопроизводства в процессе получения и использования информации с компьютерных систем и технических каналов связи

Постоянно возрастающий объем естественно-научных, гуманитарных и иных знаний на современном этапе обусловливает техническое насыщение уголовного процесса при расследовании преступлений. Усложнение криминалистических средств, используемых при выявлении, фиксации и исследовании следов преступления и доказательств, широкая инструментализация методов экспертных исследований, определяет необходимость комплекса вопросов, связанных с использованием специальных знаний участниками уголовного процесса.

Содействие специалиста в проведении предварительных исследований различных следов и материальных объектов приобретает важное значение, поскольку «облегчит и ускорит проведение криминалистических и иных судебных экспертиз» [122, 17], так как наличие у лица соответствующих специальных знаний и навыков позволит достаточно быстро и качественно выполнить необходимую работу по исследованию объектов и выявлении тех значимых моментов, которые могут быть не замечены следователем в силу отсутствия у него такой квалификации.

Специальными знаниями в уголовном судопроизводстве принято называть знания, приобретенные лицом в результате профессионального обучения либо работы по определенной специальности (п. 41 ст. 7 УПК РК). Термин «специальные знания» употребляется в уголовном процессе для обозначения любой возможной совокупности знаний (практического опыта, навыков) за вычетом общеизвестных, то есть таких, которые входят в общеобразовательную подготовку граждан, а также, исключая познания в области права. Специальные знания могут относиться к самым различным отраслям естественных и технических наук, различным видам искусства и ремесла, а также призваны для использования при решении задач уголовного процесса, направленных на быстрое и полное раскрытие преступлений, изобличение и привлечение к уголовной ответственности лиц, их совершивших. Еще раз, подтверждая актуальность участия специалистов, укажем, что специальными знаниями следователи и судьи располагают, но, как правило, в ограниченном объеме, что и послужило одной из причин создания института специалистов в уголовном судопроизводстве.

Институт сведущих лиц был известен еще в русском уголовном процессе. Так в ст. 326 Устава уголовного судопроизводства, принятого в России после судебной реформы 1864 г., говорилось: «в качестве сведущих лиц могут быть приглашены: врачи, фармацевты, профессора, учителя, техники, художники, ремесленники, казначеи и лица, продолжительными занятиями по какой-либо службе или части приобретшие особенную опытность» [123].

В отличие от Устава уголовного судопроизводства 1864 г., действующее законодательство (ст. 84 УПК РК) не регламентирует ни должностное положение, ни специальности лиц (кроме отнесения к специалистам, участвующим в следственных действиях педагога и врача), привлекаемых к участию при расследовании преступлений. Это обусловлено тем, что при современном развитии науки в многочисленных сферах деятельности человека дать исчерпывающий перечень невозможно. И как совершенно справедливо полагает П. П. Ищенко: «основной идеей, породившей институт специалистов, является использование специальных знаний для содействия следствия и суду в решении тех вопросов, в которых без их помощи сложно разобраться» [124, 3-4]. Дополняя мысль, В. Н. Махов отмечает, что «участие специалистов, как правило, повышает эффективность следственных действий, делает их более целенаправленными и полными» [125, 83].

Современным законодательством Республики Казахстан установлено, что специалистом является лицо, обладающее специальными знаниями, необходимыми для оказания содействия в собирании, исследовании и оценке доказательств, а также в применении технических средств (ч. 1 ст. 84 УПК РК).

Между тем, А. Ю. Шумилов полагает, что кроме обладания специальных знаний понятие «специалист» должно содержать наличие у него умений или навыков [34, 59]. Анализируя комментарий к Уголовно-процессуальному кодексу Казахской ССР следует отметить, что в ст. 21 также указано, что «специалист — это лицо, обладающее специальными познаниями и навыками» [126, 44]. Следует заметить, что в энциклопедическом словаре данные понятия трактуются следующим образом: «навык — это умение выполнять целенаправленные действия, доведенные до автоматизма в результате сознательного многократного повторения одних и тех же движений или решения типовых задач, а знание — проверенный практикой результат познания действительности, верное ее отражение в мышлении человека» [126, 471]. Соответственно, знание включает в себя наличие практического умения реализации теоретических знаний, и современная трактовка понятия содержит в себе определения, характеризующие лицо как специалиста.

Значимость привлечения специалистов в сфере уголовного судопроизводства подтверждается исследованием этого вопроса в криминалистических и процессуальных трудах Л. Е. Ароцкера, В. Д. Арсеньева, А. И. Винберга, Е. И. Зуева, Г. Г. Зуйкова, Г. М. Миньковского, Н. А. Селиванова, А. А. Эйсмана и других. Рассматривая использование специалистов в собирании и исследовании доказательственной информации, было отмечено, что их участие влияет на качество и своевременность расследования, а также «способствует повыше-

нию эффективности экспертных исследований, что реализуется в принципе единства и взаимообусловленности двух форм применения специальных знаний -участие специалиста и назначения производства экспертизы» [127, 54].

Говоря об интенсификации деятельности по борьбе с преступностью, следует напомнить, что она неотделима от использования достижений научно-технического прогресса, широкого применения специальных знаний, внедрения в практику расследования новейших научно-технических методов и средств. Значимость данного положения была закреплена еще в 1988 г. в приказе МВД СССР «О мерах по совершенствованию деятельности экспертно-криминалистических подразделений ОВД», где отмечено, что «умение использовать достижения науки и техники в следственной и оперативно-розыскной работе является одним из главных показателей профессиональной подготовки кадров и их способности решать поставленные задачи» [128].

В целях решения задач уголовного процесса, специалисты принимают участие не только в первоначальных следственных действиях, включаясь в тот момент, когда еще сравнительно свежи следы преступления и имеются наиболее благоприятные возможности их выявления и изъятия, но и в последующих этапах расследования, путем «оказания органам, ведущим уголовный процесс, содействия в обнаружении, закреплении и изъятии доказательств» [129, 114-117].

Следует отметить, что привлечение специалистов является не только правом (ст. ст. 221, 226, 232, 233, 235, 237-239, 257 УПК РК) органа уголовного преследования и суда, согласно ч. 1 ст. 84 УПК РК, где говорится, что «в качестве специалиста для участия в следственных и судебных действиях может быть вызвано незаинтересованное в деле лицо», но и в некоторых случаях обязанностью, согласно положениям ст. ст. 215, 224, 225, 226 УПК РК, в которых четко определена необходимость их участия. Данное мнение подтверждается выводами, отраженными в работе Ю. А. Адоян [130, 83].

Уголовно-процессуальное законодательство не предусматривает определенной формы, в которой должно выражаться требование о привлечении специалиста к производству или участию в следственных действиях. Между тем, в процессуальной литературе отмечается, что сведущее лицо приобретает процессуальный статус специалиста при:

- вынесении постановления органа (лица), ведущего уголовный процесс о производстве следственного действия;
- поручении органа (лица), ведущего уголовный процесс, о выполнении функций специалиста и разъяснения прав и обязанностей, а также предупреждения об ответственности за их невыполнение [131, 204; 132, 184].

Думается, что указанные положения требуют дополнения и разъяснения, как в части формулировки, так и по их содержанию. Так, при вынесении постановления о назначении следственного действия, условием привлечения специалиста будет не принятое решение, а указание на привлечение определенного лица для участия в следственном действии или поручение органу дознания, руководству учреждения (организации) о выделении специалиста для участия в

проводимом действии. Что и должно быть отражено в резолютивной части выносимого постановления.

Рассматривая второе положение, невольно возникает предположение, что в нем идет речь не о поручении как таковом, а об отражении в протоколе следственного действия момента разъяснения прав, обязанностей и ответственности за их невыполнение лицу, привлекаемому к участию в действии в качестве специалиста. Полагаем, что в данном случае привлечение лица для участия в проводимом действии будет осуществляться на основе повестки о вызове лица, с указанием в качестве кого оно вызывается, либо на основании запроса в учреждение, которое может выделить специалиста для разрешения интересующих вопросов, либо на основе устного приглашения в органы уголовного преследования. Данный способ позволяет привлекать лиц (специалистов) не только для участия в проведении следственного действия, но и для дачи консультаций, справочной информации.

Участие специалиста в проводимых следственных и судебных действиях, в соответствии с положением ч. 1 ст. 84 УПК РК, заключается в оказании содействия в собирании, исследовании и оценке доказательств, а также в применении технических средств. Подвергая рассмотрению обстоятельства вовлечения специалистов в сферу уголовного судопроизводства, следует отметить, что необходимость привлечения сведущих лиц обусловлена:

- отсутствием соответствующих специальных знаний и навыков у следователя, дознавателя;
- необходимостью из этических или тактических соображений поручить совершение определенных действий именно специалисту;
- одновременным применением комплекса средств криминалистической техники;
- необходимостью выполнения большого объема работы, требующей специальных познаний и навыков;
- необходимостью привлечения специальных познаний для обнаружения, исследования, фиксации, изъятия и оценки различных по природе носителей информации.

Виды помощи специалиста весьма разнообразны и зависят не только от вида проводимых действий, но и от вида специальных знаний, которыми он обладает, а также задач, которые перед ним ставятся. Анализируя участие специалистов в следственных и судебных действиях, следует отметить, что существуют определенные особенности их деятельности, которая зависит как от специфики самих процессуальных действий, так и их целей и тактических условий проведения. Анализ литературных источников [124, 10-11; 133, 43], посвященных рассматриваемой проблеме, и практики привлечения специалистов к участию в производстве следственных действий позволяет выделить основные виды задач, решаемых с помощью специалиста.

Основное назначение специалиста, участвующего в уголовном деле, является оказание содействия в:

- обнаружении и изъятии следов, предметов и вещественных доказательств;
- объяснении механизма образования следов и повреждений;
- предварительном исследовании вещественных доказательств;
- фиксации обстановки места происшествия и расположения объектов, когда это необходимо для дальнейшего исследования, в изготовлении схем, планов и другого;
- помощи полно и грамотно описать обнаруженные доказательства в соответствующем протоколе;
- помощи следователю правильно изъять и упаковать обнаруженные доказательства;
- получении образцов для сравнительного исследования;
- отборе следов и объектов, пригодных для экспертного исследования;
- подборе орудий, материалов, боеприпасов и других объектов для проведения экспериментов или опытов в процессе следственных действий;
- определении количества образцов, их качества, условий получения;
- оказании технической помощи.

Методическую помощь следователям в отработке приемов обнаружения, фиксации и изъятия доказательств сведущие лица оказывают как в рамках следственного действия, так и за его пределами. Например, в ходе осмотра компьютерной техники специалисты обучают следователей новым приемам и методам обнаружения, фиксации, изъятия информации, особенностям использования специальной техники. Однако эту же работу они проводят и на занятиях по служебной подготовке.

Задачи по оказанию консультативной помощи могут быть разрешимы всеми специалистами. Данный вид помощи заключается в разъяснениях, советах, консультациях, сообщении сведений справочного характера и тому подобном, содействующих обнаружению, фиксации и изъятию доказательств, выявлению обстоятельств, причин и условий, способствовавших совершению преступления.

Специалистами могут быть кино-, фотолюбители и звукооператоры, чертежники, инженеры-конструкторы, учителя черчения или рисования (фото-, кино-, видеосъемка, составление планов, схем, чертежей и тому подобное), программисты, системщики, альпинисты, спелеологи, монтажники высотники, аквалангисты, водолазы и другие.

Специалисты, оказывающие техническую помощь, не имеют процессуальных знаний. Но именно при оказании технической помощи данные лица производят большую часть работы самостоятельно, хотя и под руководством следователя. Данное обстоятельство должно побудить следователя перед началом следственного действия тщательно проинструктировать и по возможности обучить своих помощников основным правилам обнаружения, фиксации и изъятия следов и вещественных доказательств. Приложение специальных познаний при оказании технической помощи характеризуется отчетливо выраженной направ-

ленностью на выявление и фиксацию фактических данных в режиме производства следственных действий.

На наш взгляд, в настоящее время необходимо наибольшее внимание акцентировать на вопросах, связанных с применением научно-технических познаний сведущих лиц в уголовном судопроизводстве, как наиболее значительных для ряда других проблем. Низкая раскрываемость преступлений и качество их расследования говорят о существенных недостатках в деятельности правоохранительных органов, необходимости дальнейшего повышения ее эффективности. Причины этого заключаются как в непосредственных недостатках практики собирания и использования доказательств, так и в неразработанности некоторых основополагающих положений участия специалистов в следственных действиях и применении научно-технических познаний и средств, в зависимости от формы, в которой они используются для выполнения задач уголовного судопроизводства, а также сферы их приложения. Ограничения каждой разновидности помощи, «замыкание» их в рамках определенных параметров, носит относительный характер. Тем не менее, разграничение деятельности специалистов существенно облегчает решение многих вопросов теории и практики, связанных с использованием в уголовном судопроизводстве специальных познаний сведущих лиц, технико-криминалистических средств, научно-технических новшеств. Например, расследуя уголовное дело, следователь столкнулся с необходимостью исследования компьютерной техники, программного обеспечения и компьютерной информации. Пригласив специалиста системотехника, следователь получил исчерпывающую информацию по техническому состоянию, модели, особенностям сборки и режимам функционирования ЭВМ. Однако на вопросы, касающиеся специфики действия отдельных программ, их взаимодействия, возможности воздействия на отдельные операционные функции данный специалист ответить не смог и рекомендовал пригласить программиста, который более полно и профессионально может осветить интересующие следствие аспекты [134]. Таким образом специалисты узкопрофилирующей направленности могут оказать более профессиональную и полноценную помощь при расследовании и раскрытии преступлений.

Полагаем необходимым проанализировать и формы участия специалиста в уголовном судопроизводстве и уже исходя из установленной формы, подвергнуть анализу деятельность сведущего лица в определенной ситуации.

В комментарии к Уголовно процессуальному кодексу КазССР формы участия специалиста определены двумя позициями:

1) формы участия специалиста в уголовном судопроизводстве;
2) формы участия специалиста при производстве следственных действий [97].

Рассматривая первую позицию, следует отметить, что в сфере уголовного судопроизводства наличествуют два вида участия и привлечения к расследованию специалиста:

1) участие специалиста предусмотрено законом и его участие обязательно в следственных действиях;

2) участие специалиста предусмотрено законом в следственных и судебных действиях, однако вопрос о его привлечении решает дознаватель, следователь или судья.

В то же время следует отметить, что в научной литературе, в частности, Г. И. Повезнюк предлагает еще одну форму участия специалиста, согласно которой «специалист и его специальные знания законом не определены и не предусмотрены, и вопрос о его привлечении решает следователь и судья по-своему усмотрению» [135, 216]. Полагаем, что данная точка зрения заслуживает поддержки и закрепления в процессуальной науке и законодательстве, так как стремительное развитие науки и технологических процессов на современном этапе порождает многообразие различных форм деятельности человека, а органу уголовного преследования (при расследовании преступлений) необходима помощь специалистов самого различного профиля.

Касаясь вопроса об участии специалиста в следственных действиях необходимо отметить, что формы его деятельности таковы:

- сведущее лицо является непосредственным исполнителем действий по обнаружению, предварительному исследованию, фиксации, изъятию предметов, следов, вещественных доказательств с помощью научно-технических средств в следственных и судебных действиях. Следует согласиться с мнением Г. И. Повезнюка, что данная форма участия сведущих лиц призвана оказать срочную помощь и может выражаться в деятельности специалиста;
- по конкретному заданию (например, фотографирование места происшествия, выявить и изъять следы, установить дату и время отправки компьютерной информации с определенного компьютера и так далее);
- когда конкретное задание не дается, то есть специалист привлекается с целью общего использования его специальных знаний (например, в осмотре компьютерной техники, педагог при допросе несовершеннолетнего подозреваемого, помощь в разработке версий и в планировании расследования, а также по объему задания эксперту и правильной формулировке ставящихся перед ним вопросов и другое);
- когда специалист может самостоятельно выполнять отдельные части следственного действия (например производство перехвата сообщений, копирование и распечатка файла, освидетельствование потерпевшего, получение образцов крови и другое, естественно при соответствующем поручении следователя). Как правильно отмечает Г. И. Повезнюк, при получении информации с технических каналов связи, «следователь может и самостоятельно проработать полученную информацию, но в целях более качественного исследования, установления специфических признаков электронной документации и машинных носителей участие специалиста необходимо и незаменимо» [135, 200].

Специалист участвует в деле в качестве консультанта по разъяснению различных положений специальных знаний, интересующих орган уголовного преследования, суд, в даче рекомендаций об использовании научно-технических

средств, при проведении следственных и судебных действий и тому подобном. Например, при расследовании уголовного дела по факту неправомерного проникновения в компьютерную сеть, проведенной экспертизой был установлен компьютер, с которого осуществлялось проникновение и в качестве подтверждения сделанных выводов использовалась распечатка LOG-файлов. В целях выяснения назначения и специфики LOG-файлов и возможности использования их содержания как доказательства по уголовному делу, следователь пригласил специалиста, давшего исчерпывающую консультацию по интересующим вопросам, что в дальнейшем помогло доказать виновность лица, совершившего преступление [89].

Вопрос о гарантиях законности использования специальных знаний актуален и в связи с тем, что в юридической литературе и практике (недостаточно ясно в этом отношении и законодательство) до настоящего времени отсутствуют четкие представления о границе между участием специалиста в уголовном судопроизводстве и использованием его справочно-консультативной помощи в интересах расследования, но осуществляемой за пределами уголовного процесса. Некоторые ученые называют такую помощь самостоятельной формой использования специальных знаний и предлагают получать ее в виде показаний сведущих свидетелей, как это предусмотрено законодательством ряда зарубежных стран, например ФРГ [136, 6; 137, 24; 138].

Вместе с тем, Ю. К. Орлов отмечает, что на практике и в юридической литературе нередко встречается неверное понимание функций и процессуального положения специалиста. Он считает, что противоречивость мнений обусловлена смешением понятий специалиста в общеупотребительном смысле и процессуального положения специалиста как процессуальной фигуры и полагает, что следователь вправе получить любую консультацию у сведущего лица (как и почитать соответствующую литературу или иным образом повысить свою квалификацию), но от этого лицо не станет специалистом в процессуальном смысле. Закон предусматривает только одну форму деятельности специалиста — участие в следственном действии. Дача консультаций за рамками следственного действия — это непроцессуальная деятельность [139, 79].

Вышеизложенная информация побуждает к необходимости исследования данного вопроса и разработки положений, закрепленных в законодательстве, с целью урегулирования возникшей проблемы. Проведенный опрос респондентов (57 специалистов, 42 следователей) показывает, что на практике, в целях отражения необходимой информации в деле, специалистов обычно допрашивают в качестве свидетелей, что по существу не совпадает с их процессуальной природой, так как сведения, получаемые от сведущего лица, не образуют содержания показаний свидетеля. Такое лицо допрашивается для получения сведений консультативного, справочного характера, имеющих значение для расследования уголовного дела. Однако сотрудники следствия и дознания, используя положения Уголовно-процессуального кодекса, позволяющие допросить лицо в качестве свидетеля — «так как оно дает показания, имеющие значение для дела» — предпочитают оформлять сведения консультативного характера

протоколом допроса. Из всего массива исследованных уголовных дел, в которых специалист привлекался для участия в следственных действиях, 30 % уголовных дел содержат протокола допросов специалиста в качестве свидетеля, 10 % — справку специалиста, по 60 % исследованных дел консультативная форма участия специалиста не осуществлялась либо не документировалась.

Ссылки отдельных авторов и практиков на то, что в ст. 84 УПК РК предусмотрена обязанность специалиста давать объяснения, не учитывают того факта, что смысл этой правовой нормы совершенно конкретен и расширительному толкованию, как нам представляется, не подлежит. Статья гласит, что специалист обязан «давать пояснения по поводу выполняемых им действий». Таким образом, справочно-консультационную деятельность специалиста ни при получении информации с технических каналов связи ни в более широком смысле данная статья не предусматривает.

Исходя из этого и с учетом достаточно частого обращения следователей по уголовным делам, за таким видом помощи к сведущим лицам, считаем необходимым, ввести процессуальную регламентацию получения сведений справочно-консультативного характера.

В этой связи, заслуживает предпочтения и использования в предлагаемом решении возникшей проблемы предложение Г. К. Байжановой об оформлении консультаций специалиста в виде справок, которые будут иметь значение доказательств — «иных документов», предусмотренных ст. 123 УПК РК. Справки специалиста охватываются понятием документов, которые в соответствии со ст. 123 УПК РК признаются доказательствами, если сведения, изложенные или удостоверенные в них организациями, должностными лицами и гражданами имеют значение для уголовного дела [127, 43].

При этом полагаем целесообразным предусмотреть в необходимых случаях производство допроса специалиста с предварительным предупреждением лица об ответственности за дачу заведомо ложных показаний. Думается, что данным случаем будет являться необходимость дачи показаний специалистом, ранее участвовавшим в производстве следственного действия, по изложению обоснованности проводимых им действий, необходимости применения различных средств и разрешению других вопросов, связанных с производством следственного действия. Предлагается, в связи с возрастанием роли специалиста в получении значимой для расследования информации, ввести в УК РК статью об ответственности специалиста. Мнение, о введении в УК РК нормы, предусматривающей ответственность специалиста за дачу заведомо ложных показаний, предлагалось рядом ученых процессуалистов и криминалистов [140, 54; 141, 54; 142, 25]. В связи с чем, полагаем необходимым дополнить УПК РК нормой — ст. 217-1. «Допрос специалиста», изложив ее в следующей редакции: «если необходимо уточнить примененные специалистом методы и термины, а также выяснить ряд других вопросов, связанных с участием специалиста при проведенном следственном действии, следователь (дознаватель) вправе допросить специалиста. Перед началом допроса специалисту разъясняются его права и обязанности и он предупреждается об ответственности за дачу заведомо лож-

ных показаний по ст. 352 УК РК. Протокол допроса специалиста составляется с соблюдением правил, предусмотренных ст. 218 УПК РК.

В случае необходимости получения сведений консультативного, справочного характера, следователь (дознаватель) может пригласить специалиста для их получения. Предоставление сведений, носящих специальный характер, оформляется в виде справки, подписанной специалистом. К справке могут быть приложены схемы, таблицы, графики и другие материалы. Приложение подписывается специалистом».

Также дополнить ч. 1 ст. 352 УК РК после слов «1. Заведомо ложные показания, свидетеля, потерпевшего» словом «специалиста», и далее по тексту.

Участие специалиста в сфере уголовного судопроизводства характеризуется качеством выполнения заданий, поставленных перед ним органом уголовного преследования или судом как лицу, обладающему специальными познаниями и могущему решить вопросы специфического характера. Между тем, специалист является не единственным лицом, призванным решать вопросы с научно-технологической точки зрения. Наличие в уголовном процессе, такого участника, как эксперт, приводит к многочисленным дискуссиям относительно их деятельности с точки зрения полномочий, взаимодействия и ответственности за проводимые исследования. В связи с чем, возникает необходимость более детального рассмотрения процессуального положения специалиста и специфики осуществления его деятельности в рамках уголовного процесса.

Вопрос о компетенции специалиста тесно связан с вопросом о возможности использования специальных знаний самим следователем. По нашему мнению, основной принцип участия специалиста в следственных и судебных действиях — в практической целесообразности применения специальных знаний. Выход специалиста за пределы поставленного задания должен рассматриваться как одна из форм его инициативы, однако по некоторым моментам возможно лишь с предварительного согласия следователя.

С заданием специалисту определяются и границы его компетенции, что связано с его инициативой при производстве конкретного следственного действия. Инициатива специалиста, прежде всего, связана с полнотой использования его специальных знаний. Однако в каждом конкретном задании не всегда может быть поставлены конкретные вопросы и какая-то их часть может оказаться не предусмотренной заданием. Например, проводя осмотр компьютера обвиняемого, следователь пригласил специалиста, указав ему на необходимость исследования определенных файловых папок. Специалист же, помимо определенного ему задания, исследовал системные каталоги и обнаружил скрытые текстовые файлы, содержащие сведения, представляющие интерес для следствия. В данном случае восполнение пробелов в знаниях следователя о возможностях сокрытия информации было реализовано специалистом, благодаря наличию у него определенных специальных знаний. Во всех случаях специалист обязан довести до сведения следователя и суда о возникнувших у него определенных суждениях специального характера.

Анализ практики показывает, что известные трудности возникают при оформлении деятельности специалиста и значимости, высказываемых им мнений по поводу различных обстоятельств специального характера. Одни авторы (А. Ф. Аубакиров, А. Я. Гинзбург, А. Я. Лившиц [143], Э. Б. Мельникова [144]) сходятся во мнении, что у специалиста могут возникнуть определенные выводы, предложения, основанные на изучении фактических данных в ходе исследования материалов и применении специальных знаний. Кроме того, Ю. К. Орлов, С. Б. Бычкова считают, что «выявленные специалистом следы, изготовленные им модели, слепки, оттиски, схемы и др. результаты использования технических средств фиксации следственных действий, безусловно, имеют доказательственное значение, причем нередко весьма существенное. Другое дело, что эта деятельность фиксируется в рамках соответствующего следственного действия, а не объективизируется в отдельный, самостоятельный источник, каковым является, например, заключение эксперта» [131, 200; 139, 69].

Другие авторы (В. М. Тертышник [145, 70], Н. А. Селиванов [140, 39]) отрицают доказательственное значение мнения специалиста и его право на выводы и считают, что никаких выводов специалист делать не вправе. Если же такие им даются, то они имеют только ориентирующее значение, они не подлежат процессуальной фиксации и не могут использоваться в качестве доказательств, так как построение на основе специальных познаний выводов, имеющих доказательственное значение, является исключительной прерогативой эксперта.

По всей видимости, авторы отрицательных суждений о значимости выводов специалиста считают, что источником доказательства по закону может быть лишь вывод, основанный на применении специальных научных познаний, которые дан в форме экспертного заключения.

Проводя дальнейший анализ, из положений ст. 84 УПК РК мы видим, что данная норма не дает однозначных оснований утверждать, что специалист имеет право делать выводы. Между тем его права по исследованию материалов дела, подготовке материалов для назначения экспертизы, проведению исследований объектов предполагают, что при отражении хода и результата применения своих специальных знаний ему целесообразно высказывать мнение, давать необходимые консультации, пояснения по различным специальным вопросам. Также необходимо помнить, что ход и результаты исследования вещественных доказательств, должны найти отражение в протоколе проводимого действия либо в официальном документе, приобщаемом в качестве приложения к протоколу (ч. 8 ст. 203 УПК РК). А суд, оценивая доказательства, согласно ст. 125 УПК РК, обязан оценить все собранные доказательства в совокупности. Правильность указанного вывода подтверждается также мнением С. Ф. Бычковой, согласно которому «процессуальное закрепление результатов участия специалиста осуществляется в протоколе процессуального действия, в котором он принимал участие. При этом в протоколе отражаются: мнение специалиста; данные им консультации» [131, 200].

Рассматривая процессуальное оформление мнений, выводов специалиста и анализируя положения уголовно-процессуального закона, полагаем необходи-

мым остановиться на рассмотрении форм закрепления суждений специалиста: в протоколе следственного действия и в протоколе исследования вещественных доказательств как в официальном документе, прилагаемом к протоколу следственного действия. Анализ ч. 1 ст. 122 УПК позволяет сделать вывод о появлении нового источника доказательств — в виде протокола исследования вещественных доказательств, проведенных специалистом в ходе следственного действия. Представляется, что здесь речь идет о действии, являющимся составной частью проводимого следственного действия и закрепленного в том же протоколе в одном случае, и проведенном исследовании вещественных доказательств и закрепленном в качестве приложения к проводимому действию — в другом.

Рассматривая первый случай, следует отметить, что если проводимое специалистом исследование может быть проведено на месте обнаружения следов и вещественных доказательств и не представляет особой сложности, то есть не требуется создания лабораторных условий для получения искомых результатов и исследование может быть проведено во временных рамках проводимого действия, то сведения о произведенном исследовании объекта могут быть отражены непосредственного в протоколе следственного действия. Например, при производстве осмотра помещения (по уголовному делу № 0303200345), следователь поручил специалисту осмотреть компьютер, находящийся в квартире, а сам в это время продолжал осмотр помещения. Обнаруженная специалистом информация, по указанию следователя, была скопирована на магнитный носитель, упакована и опечатана в соответствии с установленными требованиями. Результаты проведенного осмотра компьютера были внесены в протокол осмотра и закреплены подписями участников [146].

Если же для исследования потребовались лабораторные условия, либо количество исследуемых объектов велико, то в протоколе следственного действия необходимо указать, что результаты исследования объекта будут представлены специалистом и оформлены в качестве приложения к протоколу. В данном случае, протокол исследования вещественных доказательств является «официальны документом», приобщаемом к уголовному делу в порядке, предусмотренном ч. 8 ст. 203 УПК РК, — «если в ходе производства следственного действия, по результатам исследования специалистом составлен официальный документ, этот документ прилагается к протоколу, о чем в протоколе делается соответствующая запись».

Касаясь вопроса о проводимом исследовании вещественных доказательств, следует указать, что в законе нет четкости о том, кто должен обязательно присутствовать при исследовании материалов дела специалистом, а также при составлении официального документа (следователь, понятые и другие); где специалист может проводить свои исследования: на месте обнаружения объектов или в специальных условиях, например, в криминалистической лаборатории.

Полагаем, что производство специальных исследований, проводимых в лабораторных или иных условиях, может проводиться без участия понятых, по усмотрению следователя. С точки зрения предоставления самостоятельности специалисту интерес вызывают случаи, когда сам закон допускает проводить

часть следственного действия специалисту, а следователь получает информацию о тех или иных фактах только через посредство специалиста, то есть через третье лицо. Например, освидетельствование врачом в присутствии понятых и в отсутствии следователя (п. 4 ст. 226 УПК РК). Поскольку такое положение изложено в законе, то факт определенной части следственного действия сомнений вызвать не должен. Однако следует заметить, что общее руководство действием должно осуществляться следователем и выражаться в следующем:

- детальная подготовка проводимого действия (ознакомление специалиста с планом, инструктаж);
- фиксация результатов следственного действия на фото-, видеоаппаратуре;
- организацией формы контроля (в необходимых случаях) в виде участия понятых, которые удостоверяют своей подписью ход проводимого мероприятия и его результатов.

Как справедливо отметил Г. И. Поврезнюк: «общее руководство следователя деятельностью специалиста в рамках следственного действия создает определенные ограничения процессуальной самостоятельности специалиста, однако, это не может повлиять на общую оценку, т. к. в законе четко изложена компетенция специалиста и в то же время следователь не ограничивает объем его специальных знаний и вообще применяемых научно-технических методов и средств» [135, 216]. Данное высказывание подкрепляет приказ МВД РК № 210 «О повышении эффективности применения научно-технических методов и средств в борьбе с преступностью» от 31 мая 1993 г., в котором говорится о необходимости повышения роли и ответственности экспертно-криминалистических подразделений органов внутренних дел с целью полного использования криминалистических методов и средств в борьбе с преступностью и создания надежной научно-обоснованной доказательственной базы при расследовании уголовных дел [61].

Определяя, что исследование специалиста может выступать как самостоятельный источник доказательств, основание для производства экспертизы, способ получения доказательственной информации, предлагается дополнить УПК РК ст. 251-1 «Исследование специалиста», изложив ее в следующей редакции:

«Исследование, проводимое специалистом, производится в случаях, когда обстоятельства, имеющие значение для дела, могут быть получены на основе специальных знаний, до производства экспертизы. Полученные результаты не освобождают лицо, ведущее уголовный процесс, он необходимости в соответствующих случаях назначить экспертизу.

Ход и результаты исследования отражаются в протоколе исследования вещественных доказательств, приобщаемом в качестве приложения к протоколу следственного действия (ч. 8 ст. 203 УПК РК).

Протокол исследования — письменный документ, в котором отражены выводы по вопросам, поставленным перед специалистом, основанные на результатах проведенного с использованием специальных знаний исследования. В протоколе должно быть указаны: когда, где, кем, проведено исследование,

какие материалы уголовного дела им исследованы; в рамках какого следственного или судебного действия он участвовал; какие объекты были подвергнуты исследованию; какие исследования произведены; какие методы и средства применены и в каком виде они надежны; если при исследовании специалист установит обстоятельства, имеющие значение для дела, по поводу которых ему не было изложено в задании, он вправе указать их в своем документе.

К протоколу исследования прилагаются оставшиеся после исследования объекты, а также фототаблицы, графики, модели, слепки, оттиски, схемы и другие материалы, подтверждающие выводы специалиста. Данный документ подписывается специалистом и лицами (при их участии), присутствующими при исследовании».

Настоящий вывод нашел свое подтверждение при рассмотрении вопросов участия специалиста, в рамках международного круглого стола «Проблемы развития судебно-экспертной системы РК», где Ж. Р. Дильбархановой было предложено: «считаем целесообразным внести дополнения в действующее законодательство для придания данному документу (официальный документ, составляемый специалистом) статуса самостоятельного источника доказательств» [147, 78].

3.2 Соотношение деятельности специалиста и эксперта в процессе доказывания

Уголовно-процессуальный кодекс РК (п. 5 ч. 1 ст. 96) запрещает лицу, участвовавшему в деле в качестве специалиста, в дальнейшем проводить экспертное исследование. Предыдущее участие в деле в качестве специалиста, — кроме участия врача-специалиста в области судебной медицины, является основанием для отвода эксперта. Возможность совмещения функций специалиста и эксперта широко обсуждалось в специальной литературе. Анализируя практику бывших советских республик — УССР, КазССР, Таджикской ССР и Литовской ССР, где запрет отсутствовал, отдельные ученые свидетельствовали «о его неоправданности — он не дает никаких данных, указывающих на то, что выполнение обязанностей специалистов может отрицательно сказаться в дальнейшем на объективности деятельности этого же лица в качестве эксперта по тому же делу» [139, 79; 148, 50]. На целесообразность совмещения функций специалиста и эксперта указывают также И. Л. Петрухин [149, 265] и Н. М. Кипнис [150, 128]. Справедливая критика ограничения высказывалась Г. И. Грамовичем, который указывал, что «такое запрещение невозможно обосновать ни с точки зрения принципов советского права, ни с точки зрения соблюдения интересов участников уголовного процесса» [151, 158].

Отстаивая справедливость данного запрещения, его сторонники считали, что нельзя превращать эксперта на время осмотра места происшествия в лицо, подчиненное в своих действия тому, кто производит осмотр, а затем вновь возвращать ему процессуальную самостоятельность. За недопустимость привлече-

ния в качестве эксперта лица, ранее участвовавшего в деле в качестве специалиста, высказались О. М. Глотов [152, 51], В. Н. Махов [125, 12] и другие.

Кроме обозначенной выше позиции, ученые, отстаивающие позицию запрета, полагают, что если субъект участвовал в деле как специалист, то экспертом он выступать не вправе, поскольку заинтересован в исходе дела. Предполагать, что такая заинтересованность у эксперта появится после его привлечения в качестве специалиста, на наш взгляд, нет достаточных оснований. Не следует забывать, что ч. 2 ст. 96 УПК РК прямо указывает, что «предыдущее участие лица в качестве переводчика или специалиста не является обстоятельством, исключающим их дальнейшее участие в соответствующем качестве в производстве по данному делу». Логично заключить, что законодатель не допускает появления нездорового интереса у лица лишь на том основании, что его раньше привлекали специалистом по данному делу.

Кроме того, полагаем, что данный вопрос следует рассматривать не с точки зрения негативной заинтересованности лица, а с точки позиции качества сбора исходных данных. Так, следователь, выявляя на месте происшествия следы и вещественные доказательства, фиксирует в процессуальных документах сведения, связанные с их обнаружением, состоянием, условиями изъятия и тому подобным. При этом сами следы, их индивидуальные особенности, расположение и тому подобное, как правило, фиксируются хорошо и полно. Сведения же о состоянии следа, материалах следообразующего и следовоспринимающего объектов, свойствах и особенностях отдельных материалов, изменениях, которые произошли со следами (информацией) с момента происшествия и до их обнаружения, зачастую следователем не выясняются и в процессуальных документах не фиксируются. Зафиксированная же информация носит выборочный характер, так как следователь точно не знает, что именно понадобится эксперту для исследования, что окажется важным, а что второстепенным.

Таким образом происходит утрата носителей криминалистически-значимой информации из-за того, что следователь обнаруживает и фиксирует не все необходимые для экспертного исследования объекты, а лишь часть их, представляющуюся ему важной. Если бы эксперты участвовали в производстве первоначальных следственных действий, то они помогали бы следователю отыскивать и определять эти «внутренние свойства и связи», так как эксперт гораздо лучше, чем следователь, определит механизм образования следов, взаимосвязь и взаимодействие объектов и многое другое, связанное со спецификой его деятельности. Это будет способствовать более глубокому и всестороннему исследованию экспертом следов и вещественных доказательств, которые им обнаружены, получению дополнительной доказательственной информации.

Продолжая мысль и рассматривая проблему эффективности экспертизы, напомним, что проведенное экспертное исследование окажется неэффективным, если следователь или суд представят эксперту неправильные или неполные исходные данные, снабдят его несоответствующим образом отобранными образцами, не поставят в известность об условиях, в которых были обнаружены или хранились направленные на экспертизу объекты. Например, при производ-

стве осмотра, следователь, исследуя компьютерную информацию, пытался скопировать ее на магнитный носитель, однако в связи с тем, что на диске не хватило места, он отредактировал шрифт текста и, таким образом, уменьшив объем файла, скопировал его на дискету. При исследовании данного файла эксперты не смогли ответить на ряд поставленных вопросов, так как произведенные следователем действия изменили дату, время создания файла, в связи с чем, были утрачены сведения, имеющие значение для дела [153].

Уместным будет привести точку зрения на данный вопрос начальника Бюро медицинской экспертизы А. Адашкина, который считает, что «производство экспертизы целесообразно поручать тому же эксперту, который проводил исследование. Производство экспертизы другим экспертом снижает ее эффективность, что связано с опосредованностью объекта экспертизы, с утратой и искажением части информации. Проводя практическое исследование, эксперт видит больше, чем фиксирует в Акте. Если в последующем этот же эксперт проводит экспертизу, то он несомненно больше знает, что обнаружит при этом исследовании, отчетливо представляет его особенности, детали, насколько способы, методы и приемы выполненного ранее исследования соответствуют решению поставленных вопросов. Кроме того, значительно экономится время, поскольку не требуется другому эксперту досконально изучать информацию о результатах исследования, не требуется переписывания акта в заключение, а можно сделать ссылку на него, приложив сам Акт. Следует также иметь ввиду и то, что во многих городских, районных и межрайонных отделениях экспертиз работает по 1 эксперту, что потребует привлечение специалиста из другого района, города (областного республиканского центра)» [154, 54-55].

Отстаивая позицию совмещения функций специалиста и эксперта, уместно будет акцентировать внимание на наличии существенной разницы психологического порядка в самом подходе к работе сведущего лица. Так, специалист, оказывая помощь в сборе доказательственной информации при производстве следственного действия, знает, что экспертное исследование обнаруженных следов и вещественных доказательств будет производить кто-то другой. Конечно, служебный долг обязывает, но «чужую» работу или «работу для кого-то» очень немногие делают столь же старательно. Проведенный опрос специалистов правоохранительных органов показывает, что 90 % проведенных ими исследований (без использования научных знаний) подтверждаются заключением эксперта, что свидетельствует о качестве их производства. Между тем, 60 респондентов из 70 отмечают, что эксперты, давая заключение на основе проведенного специалистом исследования (там, где не требуются лабораторные условия), не выходят за его пределы, фактически дублируя их работу. Закрепленное законодателем «недоверие» специалисту, по мнению опрошенных, не способствует проведению более углубленных исследований, могущих быть проведенными специалистом, на основе его познаний.

Продолжая анализ проблемы, отметим, что действующие нормы уголовно-процессуального закона, разрешая производство осмотра, допускают к проведению этого следственного действия лишь специалиста (ч. 6 ст. 222 УПК РК),

который затем лишен права проводить экспертное исследование собранных материалов (п. 5 ч. 1 ст. 96 УПК РК). Из этого следует вывод, что эксперта можно привлечь к участию лишь для производства экспертизы, так как его участие в качестве специалиста не позволит в дальнейшем использовать его научные познания. Опрос 50 сотрудников дознания и следствия райцентров и поселков показывает, что следователь (дознаватель) нередко вовсе отказывается от помощи эксперта в качестве специалиста, учитывая, что ему он будет необходим для производства экспертизы. Особенно часто это проявляется в отдаленных районах, где сравнительно мало сведущих лиц, могущих быть специалистами и экспертами. Реальность существования данной ситуации имеет продолжительный характер, о чем свидетельствуют аналогичные выводы, изложенные в 1975 г. Е. И. Зуевым [155, 23] и в 1981 г. И. Е. Быховским [156, 39].

Вызывает недоумение и то обстоятельство, что рассматриваемое ограничение не распространяется на судебно-медицинских экспертов. Возможно, это вызвано тем, что некомпетентность следователей в вопросах судебной медицины была очевидна с самого начала, поэтому для судебных медиков таких ограничений не предусмотрено. Полагаем, что данное обстоятельство, должно учитываться не только в сфере медицинской деятельности. Известно, что узкая специализация — удел любого развитого производства, любой современной сферы деятельности, и борьба с преступностью — не исключение. Здесь также будет продолжаться разделение труда, что приведет к повышению его производительности и качества. Уже сейчас очевидно, что осмотр трупа квалифицированнее и лучше произведет судебно-медицинский эксперт, чем следователь; осмотр компьютера — программист или техник, специализирующийся на сборке компьютерной техники или ее диагностике и так далее. Участие специалистов узкой направленности в процессе расследования прежде всего связано с современным развитием информационно-телекоммуникационных систем, основными составляющими которых являются физические каналы передачи информации различной природы (эфирные, проводные, волоконно-оптические линии связи и высокочастотные линии электропередачи), а также создание аппаратуры каналообразования и коммутации. Нехватка специалистов в данной области ставить перед необходимостью рассмотрения вопроса о привлечении сведущих лиц (узкой направленности) как для участия в производстве экспертиз, так и в качестве специалистов на предварительном следствии.

Актуальность данного вопроса находит свое отражение в практической деятельности органов следствия и дознания. Анализ уголовных дел показывает, что нередки случаи, когда эксперты не могут дать заключение, а проводимые специалистами исследования тех же объектов дают положительное заключение и позволяют изобличить преступников. В связи с чем, сложилась практика проведения совместных экспертных исследований [157]. Как справедливо отмечает С. П. Вареникова: «потребности судебно-следственной практики в получении доказательственной информации при изучении новых, не встречавшихся ранее объектов, обусловливают появление в классификации новых классов, родов и

видов судебных экспертиз. Это в свою очередь, диктует необходимость расширения сферы специальных знаний судебных экспертов» [158, 96].

Рассматривая аспект узкой специализации и уникальности сведущих лиц, полагаем необходимым исследовать вопрос участия специалистов в производстве экспертизы, так как положение ст. 243 УПК РК позволяет в разовом порядке проводить экспертизу иным лицам, отвечающим требованиям ч. 1 ст. 83 УПК РК. Кроме незаинтересованности и обладания специальными научными знаниями, уголовно-процессуальный закон позволяет осуществлять производство экспертизы другим лицам, требования к которым определяются законодательством РК, но не указаны в Уголовно-процессуальном кодексе, что определяет перед нами задачу анализа и раскрытия данного положения.

В ст. 10 Закона РК «О судебной экспертизе» от 12 ноября 1997 г. № 188, с изменениями от 5 мая 2000 г. и от 6 ноября 2001 г., определено, что производство судебной экспертизы может быть поручено: сотрудникам органов судебной экспертизы; лицам, осуществляющим судебно-экспертную деятельность, на основании лицензии, в разовом порядке иным лицам [159]. Под лицензией понимается выдаваемое компетентным государственным органом разрешение гражданину или юридическому лицу заниматься определенным видом деятельности или совершать определенные действия [160]. При этом указано, что производство экспертизы в разовом порядке может быть поручено в случаях:

1) назначения экспертизы, не предусмотренной определенным законодательством перечнем видов экспертиз;
2) привлечения в качестве эксперта специалиста иностранного государства в области судебной экспертизы, в соответствии со ст. 27 Закона РК «О судебной экспертизе»;
3) удовлетворения отводов всем экспертам соответствующей специальности, являющимся сотрудниками органов судебной экспертизы, а также осуществляющим судебно-экспертную деятельность на основании лицензии (на производство экспертизы), либо мотивированного отстранения от производства экспертизы этих лиц и соответствующего органа [159].

Подвергая анализу первый случай, мы имеем полное основание полагать, что здесь законодатель имеет в виду узкую направленность какой-либо отрасли и необходимость привлечения специалистов редкостных профессий в целях разрешения вопросов, поставленных перед экспертами. Возможность привлечения специалистов в данной ситуации подтверждается положениями 5, 8 «Инструкции о порядке производства судебных экспертиз в КазНИИ судебных экспертиз», согласно которым «если требуются познания в различных отраслях науки и техники, организуется проведение комплексной экспертизы. Для ее производства назначаются специалист(ы) соответствующих отраслей знаний. С согласия лица, назначившего экспертизу, к ее производству могут привлекаться также специалисты, не являющиеся штатными сотрудниками Института. Во время производства экспертизы на них полностью распространяются требования Инструкции» [161].

В случае же непривлечения сведущих лиц, мы столкнемся с ситуацией, когда отсутствие соответствующих специалистов или оборудования (например, при разрешении вопросов, связанных с природой фактических данных, полученных с использованием ЭВМ и ряда других) повлечет возвращение материалов экспертизы лицу, ее назначившему и (или) направление их в другое экспертное учреждение, если оно сможет разрешить данную проблему. Изложенный вид решения предусмотрен в вышеозначенной Инструкции. Думается, что исходя из задач уголовного судопроизводства, в частности, направленных на быстрое и полное раскрытие преступлений, данная ситуация нежелательна и необходимость привлечения специалистов говорит сама за себя.

Проведение судебной экспертизы с привлечением судебных экспертов иностранного государства, полагаем, что также связано с отсутствием либо малочисленностью (и как следствие, большой загруженностью) экспертов в государстве. Следует отметить, что правом привлечения судебного эксперта иностранного государства обладает орган (лицо), ведущий уголовный, процесс, а также руководитель органа судебной экспертизы с согласия органа (лица), назначившего экспертизу. Проведение судебной экспертизы с участием судебного эксперта иностранного государства осуществляется в соответствии с уголовно-процессуальным законодательством Республики Казахстан. Думается, что привлечение иностранных экспертов может быть обусловлено лишь критически сложившейся ситуацией, так как оно влечет большие финансовые затраты, а также не может в полной мере обеспечить тайну следствия и нераспространенность различного рода сведений. Необходимость сохранения в тайне сведений может быть связана с их специфичностью, например: государственные секреты Республики Казахстан, информация оперативного характера, либо сведения, имеющие отношение к деятельности специальных органов (например, КНБ) и другое.

Рассматривая третий случай возможности поручения специалистам производства экспертизы, законодатель обуславливает эту необходимость удовлетворением отводов, заявленных экспертам и как следствие исключение возможности поручения последним производства судебной экспертизы.

Кроме обстоятельств, предусмотренных уголовно-процессуальным законодательством Республики Казахстан (глава 11 УПК) и являющихся основанием для отвода, Закон РК «О судебной экспертизе» устанавливает, что лицу не может быть поручено производство экспертизы если оно:

- признанно в установленном законом порядке ограниченно дееспособными и недееспособными;
- ранее судимо;
- уволено по отрицательным мотивам с должности, связанной с осуществлением судебно-экспертной деятельности [159].

Еще раз подтверждая значимость деятельности специалистов в различных сферах деятельности государства, приведем в качестве примера положения главы 3 Постановления Правительства РК «Об утверждении Правил импорта, экспорта, реализации и использования специальных технических средств для про-

ведения специальных оперативно-розыскных мероприятий, а также специальных материалов и оборудования для их производства в РК», согласно которым привлечение специалистов и независимых экспертов производится в случаях:

- возникновения необходимости в специальных познаниях;
- возникновения необходимости в проведении независимой экспертизы [162].

Подводя итог проведенному анализу мы полагаем, что обсужденное ограничение является преградой на пути широкого использования современных возможностей судебной экспертизы в борьбе с преступностью и ведет к нарушению принципа непосредственности восприятия обстановки места происшествия, в целом, и вещественных доказательств в их первоначальном виде, в частности. Кроме того, информация о событии преступления, имевшаяся на месте происшествия, попадает к эксперту через вторые, а иногда и третьи руки, что вызывает ее искажение и утечку.

Стремительное развитие технологической сферы (вкупе с другими) на современном этапе обуславливает необходимость вовлечения сведущих лиц различной категории в сферу уголовного судопроизводства, как для участия в следственных действиях, так и для производства экспертиз. Уникальность специалистов быстротечно развивающихся направлений (например, в области разработки и применения специальных технических средств для перехвата и регистрации информации с технических каналов связи, компьютерных систем и иных технических средств, а также технических и программных средства для оснащения компьютеров и компьютерных систем, позволяющие производить многоканальную регистрацию (запись) телефонных переговоров) говорит о проблеме производства отдельных видов экспертиз и обуславливает расширение возможности участия экспертов (специалистов) в производстве следственных действий.

В подтверждении изложенных нами позиций отметим, что назревшая необходимость усиления роли специальных знаний, в том числе судебной экспертизы, как основной формы их применения, в объективизации процесса доказывания по уголовным делам стала предметом пристального внимания участников круглого стола «Проблемы развития судебно-экспертной системы РК», которыми по итогам обсуждения были определены следующие рекомендации: «рассмотреть вопрос о совершенствовании процессуального статуса специалиста в судопроизводстве, а также о процессуальной форме результатов его деятельности; провести обучение ряда сотрудников органов судебной экспертизы по судебным инженерно-технической, компьютерно-технологической и экономической экспертизам в рамках второго высшего профессионального образования на базе ВУЗов РФ». Следует отметить, что в 2003 г. прошли обучение и получили специальности 187 экспертов, прошли стажировку с присвоением дополнительной специальности 112 человек [147, 109-110].

В связи с чем, полагаем целесообразным отказаться от запрета на совмещение функций специалиста и эксперта и дополнить нормы Уголовно-процессуального кодекса РК следующими положениями.

Дополнить ч. 1 ст. 96 УПК РК «Отвод эксперта», пунктами:

«6) если он признан в установленном законом порядке ограниченно дееспособными и недееспособными;

7) если он ранее судим;

8) если он уволен по отрицательным мотивам с должности, связанной с осуществлением судебно-экспертной деятельности».

Изменить п. 3 ч. 1 ст. 243 УПК РК «Лица, которым, может быть поручено производство судебной экспертизы» и изложить в следующей редакции:

«3. в разовом порядке в случаях:

- назначения экспертизы, не предусмотренной определенным законодательством перечнем видов экспертиз;
- привлечения в качестве эксперта специалиста иностранного государства в области судебной экспертизы, в соответствии со ст. 27 Закона РК «О судебной экспертизе»;
- удовлетворения отводов всем экспертам соответствующей специальности, являющимся сотрудниками органов судебной экспертизы, а также осуществляющим судебно-экспертную деятельность на основании лицензии (на производство экспертизы), либо мотивированного отстранения от производства экспертизы этих лиц и соответствующего органа».

Исключить п. 5 ч. 1 ст. 96 УПК РК: «Если он участвовал в деле в качестве специалиста, за исключением случаев участия в соответствии со ст. 224 настоящего кодекса врача-специалиста в области судебной медицины в осмотре трупа человека».

3.3 Особенности назначения судебно-экспертного исследования компьютерных систем и заключенной в них информации

При осуществлении перехвата сообщений компьютерные системы и технические каналы связи являются носителями информации, которая вовлекается в сферу уголовного судопроизводства и является объектом исследования. С целью вовлечения информации в процесс доказывания она подлежит исследованию, с позиций относимости, допустимости и достоверности. Определение вышеуказанных свойств информации делает ее объектом судебной экспертизы, которая позволяет выявить ряд свойств исследуемой информации и решить вопрос о ее дальнейшей судьбе.

Многопрофильность применения компьютерной техники, ее совершенствование, появление новых систем для сохранения и передачи информации, обусловливает проблемность производства программно-технических или информационно-технических экспертиз, системой государственных органов судебной экспертизы Республики Казахстан, включающей:

- Центр судебных экспертиз Министерства юстиции Республики Казахстан и его территориальные подразделения;
- Центр судебной медицины Министерства здравоохранения Республики Казахстан и его территориальные подразделения;

- Специализированные подразделения государственных органов, к функциям которых отнесено производство судебной экспертизы в соответствии с законодательством Республики Казахстан [159].

Слабая программно-техническая база специальных лабораторий и апробирование отечественными учеными методик подобных исследований способствовали привлечению специалистов соответствующей квалификации извне экспертных учреждений, определенных выше, для участия в производстве судебной экспертизы на основании разовых разрешений, выдаваемых в порядке, установленном законодательством. Полагаем, что в отдельных случаях, когда в специальных экспертных учреждениях отсутствуют направления по производству различного вида экспертиз, связанных с исследованием компьютерной техники и программного обеспечения, необходимо предусмотреть возможность производства указанной экспертизы вне государственных экспертных учреждений. К примеру, следственные органы МВД РФ в настоящее время идут по пути назначения программно-технических экспертиз в подразделениях ФАПСИ, либо привлекают для производства такого рода экспертиз специалистов соответствующих квалификаций извне экспертных учреждений, поскольку в системе МВД РФ не имеется экспертов, проводящих подобные исследования [163; 164, 7]. Так, если в 2000 г. производство экспертиз информационных технологий проводилось в 6 судебно-экспертных учреждениях, то в 2001 г. — уже в 8 СМУ [165, 69]. Значимость своевременного производства различного вида экспертиз (генная, видео- и аудиоидентификационная, компьютерно-технологическая и другие), и как условие этого — отработанная методика ее осуществления, проявляется и в том, что сроки расследования по большому числу дел затягиваются из-за задержек в учреждениях судебной экспертизы. И несомненно, что заключения указанных экспертиз (многие из которых уже получили интенсивное развитие за рубежом [166, 54]) имеют серьезное значение при расследовании наиболее сложных дел и принятии обоснованных процессуальных и судебных решений.

Между тем, проблема разработки соответствующих методик экспертного исследования средств компьютерной техники остается жизненной и актуальной, так как отечественная практика и наука в этом отношении, в настоящее время, находится на стадии формирования и не имеет возможности привести наработанные практикой методики исследования. В связи с чем, полагаем необходимым обратиться к опыту зарубежных стран, рассматривавших эту проблему на основе научного исследования при использовании конкретных практических наработок правоохранительных органов. Так, в марте 1993 г. в Российской Федерации в г. Москве прошло очередное занятие постоянно действующего межведомственного семинара на тему «Криминалистика и компьютерная преступность», организованное координационным бюро по криминалистике при НИИ проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и экспертно-криминалистическим центром МВД РФ. На данном семинаре были рассмотрены вопросы назначения, проведения, возможностей экспертных исследований, характерных для преступле-

ний, совершаемых с использованием компьютерной техники. Так, Ю. Батурин предложил создать банк данных, применительно к различным группам компьютерных программ и объектов компьютерной техники, которые могут существенно облегчить их групповую идентификацию. А также разработать критерии, посредством которых можно определять, достаточен ли объем конкретной программы (например, по числу команд или качеству использованных алгоритмов) для использования ее в качестве сравнительного образца. Весьма интересная идея была выдвинута Е. Белоглазовым. Им была предложена мысль о целесообразности разработки методики экспертного исследования с целью идентификации пользователя ЭВМ при возникновении версии о том, что определенное лицо произвело какие-либо манипуляции с машинной информацией. Суждение о возможности такого отождествления, по мнению автора этой идеи, основано на том, что комплекс периодов времени нажатия пользователя ЭВМ на различные клавиши терминала можно рассматривать как своеобразный «таймерный почерк». При условии его фиксации в компьютере он может способствовать определению классификационной группы, к которой относится искомый пользователь, а в некоторых благоприятных случаях и индивидуализировать его. Конкретно Е. Белоглазов предложил разработать: методику установления соответствия определенного компьютера стандарту и проверки его работы (с помощью специальных тестов), методику исследования компьютерных вещественных доказательств, предусматривающую, в частности, фиксацию источника, вида, способа ввода, вывода данных и их обработку [167].

Исследуя вопросы назначения, проведения возможностей экспертных исследований, характерных для преступлений, совершаемых с использованием компьютерной техники, Н. Селиванов [168, 36] и Ю. Батурин [169, 271] предложили концепцию идентификации автора компьютерной программы, основанную на использовании в качестве общего идентификационного признака степени выработанности у составителя программы профессионального навыка, а в качестве частных признаков — используемых в автороведческой экспертизе синтаксических, лексических особенностей письменной речи, а также топографических признаков (форма левого поля текста программы, особенности выделения фрагментов абзацами).

Анализ разработки методики экспертного исследования средств компьютерной техники проводился и казахстанским ученым Р. А. Назмышевым [110, 130] и, соглашаясь с его выводами, представляется возможным выделить три основные направления методики экспертного исследования:

- создание банка данных различных типов компьютерных программ с целью их идентификации при возникновении такой необходимости, главным определяющим моментом, в чем является их сравнение по числу заложенных в каждой из них числа команд и качеству использованных алгоритмов;
- разработка методики экспертного исследования средств компьютерной техники с целью идентификации пользователя ЭВМ (правонарушителя), где критерием для его поиска является определение периода вре-

мени нажатия им клавиш терминала, определения скорости работы на ЭВМ и использование этих данных для отождествления личности правонарушителя;

- разработка методики экспертного исследования с целью возможности осуществления поиска пользователя ЭВМ (правонарушителя) по степени выработанности у него профессиональных навыков, частными критериями чего может являться синтаксические, лексические и топографические признаки и особенности его работы на ЭВМ (разработка программ, работа с текстом программы и так далее).

Несмотря на оригинальность предлагаемых указанными выше авторами идей и концепции, направленных на возможность идентификации пользователя ЭВМ, в особенности двух последних, считаем, что по некоторым субъективным факторам процесс идентификации пользователя ЭВМ (правонарушителя) может быть усложнен. К таким факторам, способным осложнить исследование и исказить его результаты по обозначенным двум последним методикам, может быть отнесено следующее: стресс, опьянение оператора, попытки имитировать навыки другого лица, ограничение зрительного контроля, психическое состояние пользователя и другое.

На основе анализа изложенного, представляется возможным сделать вывод о том, что при разработке методик экспертного исследования средств компьютерной техники, важно, чтобы ее разработчики имели углубленные знания об архитектонических свойствах и особенностях компьютерной техники и ее средств. А для возможности установления различных аспектов (распознавания периода и времени нажатия на клавиши терминала, определения профессиональных навыков пользователя ЭВМ и так далее): «необходимо, прежде всего, наличие специальных компьютерных программ, а также высококлассное оборудование и качественное оснащение помещений, в которых осуществляется производство судебной экспертизы» [170].

Продолжая рассмотрение вопроса, обозначив существующие проблемы и частичного их анализа, обратим внимание на специфичность постановки вопросов и особенностей назначения экспертиз в сфере компьютерных технологий. В число экспертиз, производимых в центре судебной экспертизы Министерства Юстиции Республики Казахстан, входит судебно-экспертное исследование средств компьютерной технологии. Данный вид экспертизы указан как судебно-технологическая. Между тем, в ряде научной [171, 204] и специальной литературы (в том числе зарубежной) [172, 224] данный вид экспертизы носит название компьютерной, что в целом не противоречит существу ее производства и полагаем не повлияет на восприятие ее содержания и методики производства.

По мнению Г. И. Поврезнюк: «судебно-компьютерная экспертиза — представляет собой новый вид судебный экспертизы, необходимость которой обуславливается широким внедрением компьютерной техники и технологий практически во все сферы человеческой деятельности» [173, 144-147]. Задачи, ре-

шаемые компьютерно-технической экспертизой, делятся на диагностические и идентификационные [173, 254]:

а) диагностические задачи (или задачи общего системного анализа):

- диагностика и классификация систем (например, классификация компьютерной системы (принтера, факса, копира) по тексту, изготовленному с ее применением; отнесение информации к категории программного обеспечения ЭВМ);
- определение структуры и функций систем; определение элементов системы и ее границ;
- анализ системных норм; определение семантики и прагматики спорных текстов, работы неизвестных компьютерных систем, воздействия деятельности систем на окружающую микро- и макросреду;
- реконструкция и прогнозирование поведения систем;
- определение надежности и устойчивости компьютерных систем; отнесение конкретных программ к вредоносным;
- реконструкция ОМП методами математического анализа и компьютерного моделирования;
- криминалистическая диагностика роли и функционального назначения отдельных элементов компьютерной системы, диагностика межэлементных связей и отношений;
- криминалистическая диагностика системных процессов и поведения систем;

б) идентификационные задачи:

- идентификация системы;
- идентификация автора машинного текста;
- системный анализ обстановки места происшествия (ОМП);
- диагностика интеллектуального взлома системы.

Приведенные ниже положения, касающиеся предмета, объектов, метода исследования и перечня, ставящихся перед экспертом вопросов, основаны на изучении ряда специальной [174, 145; 175, 44] и научной [65, 276; 176, 246-251; 177, 264] литературы и заключаются в следующем.

Предметом судебной экспертизы средств компьютерной технологии являются обстоятельства дела, связанные с установлением:

- конструктивных особенностей и технического состояния компьютеров и периферийных устройств;
- информации, содержащейся в оперативной памяти компьютера и на магнитных носителях;
- способов изменения компьютерных программ.

Объектами судебно-компьютерной (технологической) экспертизы могут являться:

- компьютеры в сборке и их системные блоки;
- компьютерные системы (компьютерные сети);
- периферийные устройства (дисплеи, принтеры, дисководы, модемы, клавиатуры, сканеры, манипуляторы, джойстики и так далее);

- коммуникационные устройства компьютеров и вычислительных систем;
- технические средства и магнитные носители информации (жесткие, флоппи-диски, оптические диски, ленты), множительная техника, средства спецтехники и связи;
- электронные записные книжки, пейджеры, иные носители текстовой или цифровой информации, техническая документация к ним распечатки программных и текстовых файлов;
- словари поисковых признаковых систем, классификаторы;
- документы, изготовленные с использованием компьютерных систем и электронных средств передачи и копирования информации (факсы, ксерокопии и так далее);
- компьютерная информация (программы, тексты);
- программное обеспечение различных форм, типов, видов, функционального назначения и способов исполнения;
- документы (договоры на покупку, создание (передачу) научно-технической продукции; калькуляции стоимости этапов предпродажной подготовки компьютеров; сопроводительная документация к компьютерной, вычислительной технике; справочные данные; инструкции пользователя и другое);
- системные процессы обмена информацией и связи между элементами компьютерных систем;
- видео- и звукозаписи, визуальная и аудиоинформация, в том числе на лазерных дисках;
- материалы дела, относящиеся к предмету экспертных исследований.

Основными методами исследования таких объектов являются квалифицированное наблюдение, системный анализ, математическое моделирование, инструментальный анализ с применением ЭВМ, статистический и социальный эксперимент, метод экспертных оценок, специальные методы предметных наук.

Определив объекты судебно-технологической экспертизы, напомним, что отправляемые на экспертизу магнитные носители, компьютеры и (или) периферийные устройства, должны быть тщательно упакованы, дабы не допустить повреждения или уничтожения искомой информации. Для упаковки могут использоваться как специальные футляры, так и обычные бумажные и целлофановые пакеты, исключающие попадание грязи и тому подобного на рабочую поверхность дискеты или магнитной ленты. Каждое устройство компьютера и соединительные кабели упаковываются в специально подготовленный плотный упаковочный материал. Учитывая важность информации содержащейся в системном блоке, необходимо его опечатать перед упаковкой в специальный плотный материал — заклеить лентой кнопку включения компьютера и гнездо для подключения электрокабеля, а также места соединения боковых поверхностей с передней и задней панелями и далее опечатать материал, который был упакован в этот системный блок.

В качестве примера неосмотрительного отношения к хранению магнитных носителей можно отнести случай, когда следователь положил на магнит на дискеты, лежащие на столе без упаковочного материала и вся имеющаяся информация на них была утрачена.

Направляя объекты на исследование, в целях разрешения ряда вопросов, ответы на которые могут быть связаны с особенностями местонахождения изъятой техники, следователю необходимо также направить экспертам протоколы (или их копии) обыска, выемки или осмотра.

В соответствии с задачами исследования судебно-компьютерную экспертизу можно разделить на два вида:

1) техническая экспертиза компьютеров и их комплектующих (конструкция компьютера, магнитных носителей, компьютерных сетей и их работа);
2) экспертиза программного обеспечения (исследование информации, хранящейся в компьютере и на магнитных носителях).

В результате производства судебно-экспертного исследования средств компьютерной технологии, как это следует из специальной литературы, перед экспертом могут быть поставлены вопросы, сформулированные следующим образом.

При решении диагностических задач при проведении технической экспертизы компьютеров и их комплектующих:

- К какой модели, типу относится представленный на исследование компьютер?
- Каковы технические характеристики системного блока и периферийных устройств данного компьютера?
- Соответствуют ли функциональные и технические возможности представленного компьютера и периферических устройств, прилагаемой к ним технической документации и условиям, оговоренным в договоре поставки?
- Какова причина неисправности представленного компьютера? Не является ли ее причиной перепад напряжения в сети, резкое отключение электроэнергии, механическое воздействие на корпуса функциональных блоков, произведенные монтажно-наладочные работы?
- Каковы технические характеристики конкретной вычислительной сети?
- Каковы функциональные возможности представленного компьютера в комплекте с имеющимися периферийными устройствами?
- Какая операционная система использована в данном компьютере?
- Где и в какое время собран данный компьютер и его комплектующие?
- Каково назначение данного предмета, возможность его использования?
- Подвергался ли представленный компьютер разукомплектованию?
- Какие конструктивные особенности он имеет? Из каких частей он состоит? Промышленным или кустарным способом изготовлен?

- Если предмет изготовлен кустарным способом, то познаниями, в какой области науки, техники и ремесла обладает лицо, изготовившее указанный предмет, каков уровень профессионализма указанного лица?
- В совокупности, с какими предметами и приборами может быть использован данный предмет?
- Каковы технические характеристики данного предмета? Возможности его использования.
- Каковы технические характеристики иных электронных носителей информации? Исправны ли они? Каковы причины неисправностей?
- Не содержат ли магнитные носители информации физических дефектов?
- Имеют ли комплектующие компьютера единый источник происхождения (печатные платы, магнитные носители, дисководы)?
- Соответствует ли внутреннее устройство компьютера и его периферии прилагаемой технической документации?
- Не внесены ли в конструкцию компьютера какие-либо изменения?
- Исправен ли данный компьютер и его комплектующие?
- Какова степень износа компьютера и его комплектующих?
- Каков процент износа определенной детали компьютера?
- Какова причина неисправности компьютера и периферийных устройств?
- Имеют ли магнитные носители информации какие-либо физические дефекты?
- Не производилась ли переделка (адаптация) компьютера для работы на нем специфических пользователей (человек со слабым зрением, левша и другое)?
- Каковы технические характеристики иных электронных средств (пейджер, телефонный сервер) приема, накопления и передачи информации?
- Какое время необходимо для копирования представленной информации на представленный носитель магнитной информации?
- При каких условиях возможно снятие информации с исследуемого компьютера?
- Имеет ли исследуемый компьютер вход в систему «Интернет», если имеет, дать его характеристику

При решении идентификационных задач при проведении технической экспертизы компьютеров и их комплектующих:

- Имеют ли комплектующие компьютера единый источник происхождения?
- Каковы конфигурация и состав компьютерных средств и можно ли с помощью этих средств осуществить действия, инкриминируемые обвиняемому?

При экспертизе программного обеспечения и компьютерной информации и решении диагностических задач могут быть сформулированы следующие вопросы:

- Какая операционная система использована в данном компьютере?
- Имеется ли на жестком диске представленного на исследование компьютера информация, соответствующая представленному образцу?
- Каково содержание информации, имеющейся на внутренних и внешних магнитных носителях (базовое математическое обеспечение, программы СУБД, АРМ и другие)?
- Каковы функциональное назначение, характер, содержание информации, имеющейся на представленном для исследования компьютере (носителе магнитной информации)?
- Каково назначение программ, находящихся в компьютере, каков алгоритм их функционирования? Способ ввода и получения информации?
- Имеются ли на представленных магнитных носителях специализированные программы, используемые для подбора паролей либо иного незаконного проникновения в компьютерные сети? Если да, то каковы их названия, особенности работы, возможности использования для проникновения в конкретную компьютерную сеть?
- Имеются ли признаки, свидетельствующие о применении конкретной программы для незаконного проникновения в выше указанную сеть? Если да, то какие?
- Какова хронологическая последовательность необходимых действий для запуска конкретной программы, либо совершения определенной операции?
- Возможно ли, работая в данной компьютерной сети произвести в среде программных продуктов какие-либо изменения программных файлов? Если возможно, то, какие, каким образом и с какого компьютера могут быть произведены подобные изменения?
- Являются ли данные программные продукты лицензионными или несанкционированными копиями стандартных программ либо оригинальными разработками?
- Не внесены ли в данный программный продукт какие-либо коррективы, изменяющие выполнение некоторых операций?
- Соответствует ли полученный программный продукт техническому заданию (указать, какому)?
- Возможно ли использование представленной программно продукции для выполнения определенных задач?

При наличии на ЭВМ пароля доступа перед экспертами могут быть поставлены следующие вопросы:

- Имеет ли ЭВМ пароль на всю информацию или только на ее определенную часть?
- Использовались ли для ограничения доступа к информации пароли, скрытые файлы, программы защиты?

- На какие программы распространяется действие вируса?
- Какую информацию содержат предъявленные на экспертизу системные блоки и дискеты?
- Какую информацию содержит файл «… имя.doc»?
- Имеются ли в компьютере данные, доступ к которым ограничен использованием паролей, скрытых файлов, программ защиты и так далее)?
- Возможно ли снять пароль и прочитать информацию?
- Каково содержание скрытой информации?
- Каково содержание информации, находящейся в зашифрованном файле, поименованном «….» на носителе магнитной информации?
- Предпринимались ли попытки подбора паролей, взлома защитных средств или иные попытки несанкционированного доступа к закрытой информации?
- Осуществлялся ли несанкционированный доступ к компьютерной информации, содержащейся на ... ?
- Возможно ли получить доступ к конфиденциальной информации, имеющейся в указанной сети?
- Каким образом осуществляется такой доступ?
- Имеется ли возможность с представленного компьютера, получить доступ к указанной сети?
- Каким образом осуществлено вхождение пользователя в указанную локальную сеть?
- Каковы признаки, свидетельствующие о таком вхождении?
- Если незаконное проникновение произошло извне, то какие имеются возможности по идентификации компьютера, с которого произошло проникновение?
- Если отсутствуют признаки вхождения в сеть стороннего пользователя, указать, с каких компьютеров можно произвести подобные операции?
- Содержатся ли на предъявленных системных блоках и магнитных носителях текстовые файлы? Если да, то, каково их содержание и возможность использования?
- Подвергалась ли данная компьютерная информация уничтожению, копированию, модификации, блокированию?
- Имеется ли уничтоженная информация на представленных магнитных носителях? Возможно ли ее восстановление? Если да, каково ее содержание, возможности использования?
- Установить время с момента ввода данных до получения результатов при работе данной компьютерной программы?
- Имеется ли утечка информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных, если да, то какова ее природа?
- Имелись ли (имеются) сбои в работе компьютера и отдельных программ, каковы причины этих сбоев?

- Какие правила эксплуатации ЭВМ существуют в данной информационной системе, и были ли нарушены эти правила?
- Находится ли нарушение правил эксплуатации ЭВМ в причинной связи с уничтожением, копированием, модификацией или блокированием информации?
- Нарушение каких правил эксплуатации компьютерной системы привело к потере информации на ней? Можно ли восстановить информацию?
- Не являются ли представленные файлы с программами зараженными вирусом, и если да, то каким именно?
- Не является ли причиной сбоев в работе компьютера наличие вируса?
- Возможно ли восстановить в полном (частичном) объеме функционирование данной программы, поврежденной вирусом?
- Каково содержание информации, хранящейся на пейджере, в электронной записной книжке?
- Когда созданы (произведено последнее изменение) данных на представленном для исследования носителе магнитной информации?

В отношении определенных файлов могут быть сформулированы вопросы:

- Когда создан данный файл?
- Сколько файлов создано «__» числа и какова их судьба? (удалены или нет, если отправлены по почте, то на какой адрес и когда)?
- Можно ли установить, на какой ЭВМ, создан данный файл? Каковы его атрибуты, свойства?
- Изменялось ли содержание файла? Если да, то сколько раз, дата и время внесения последних изменений.
- Когда и с какого адреса были получены данные файлы?
- Когда проводилась последняя корректировка данного файла (инсталляция конкретного программного продукта)?

При решении идентификационных задач:

- Каковы технические характеристики аппаратных средств, необходимых для изготовления представленного на исследование документа ...?
- Кем создана данная компьютерная программа?
- Могла ли данная компьютерная программа быть создана конкретным специалистом?
- Каков уровень профессиональной подготовки в области программирования и работы с компьютерной техникой человека, производившего данные действия с компьютером и программным обеспечением?
- Возможно ли установить уровень профессиональной подготовки в области программирования и работы с компьютерной техникой лица, работающего с компьютером?
- Каков способ изготовления представленных документов (программ, текстов, данных иного формата)?
- Не являются ли обнаруженные файлы копиями информации, находившейся на конкретной ЭВМ?

- Не являются ли представленные тексты на бумажном носителе записями исходного кода программы и каково назначение этой программы?
- Какие программные и технические средства использованы при изготовлении представленного на исследование документа ...?

Перед назначением экспертизы формулировки вопросов целесообразно согласовать с экспертом.

Приведенный перечень вопросов в зависимости от совокупности собранных по делу фактических данных и обстоятельств, которые необходимо установить, может быть расширен и дополнен новыми вопросами.

Учитывая специфичность исследования, для разрешения ряда вопросов не технического характера, возможно совмещение программно-технической экспертизы с другими. Например, с автороведческой, объектами исследования которой являются письменные содержания документов (письменная речь). Автороведческая экспертиза проводится для решения следующих основных задач:

- установление автора документа по письменной речи;
- определение уровня грамотности автора документа.

На разрешение автороведческой экспертизы могут быть поставлены следующие вопросы:

- Является ли автором документа конкретное лицо?
- Является ли автором нескольких документов одно лицо?
- Каковы уровень грамотности и степень владения навыками письменно-речевого характера у автора документа?

Для установления автора документа необходимо направить:

- исследуемый документ с точным указанием реквизитов и других его особенностей;
- свободные образцы письменной речи в количестве 10-15 документов (рукописного, машинописного, полиграфического характера), составленные проверяемым лицом вне связи с рассматриваемым событием (письма, черновики, личные записи в дневниках, автобиографии, докладные, объяснительные записки, рапорты и так далее);
- свободные образцы письменной речи проверяемого лица должны быть выполнены в рамках того же функционального стиля и в той же письменной речи, что и исследуемый документ;
- экспериментальные образцы письменной речи должны быть представлены в виде сочинений (изложений), выполненных проверяемых лицом на самостоятельно им избранную или предложенную следователем тему. Необходимо знать, что экспериментальные образцы, выполненные под диктовку, не могут быть использованы в качестве полноценного сравнительного материала.

Продолжая вопрос исследования компьютерной техники и технологий, следует отметить, что большую помощь в исследовании аппаратных и программных средств компьютерной техники оказывают специалисты информационно-вычислительных центров региональных УВД МВД России. Например, в

системе МВД начато производство так называемых программно-технических экспертиз, которыми могут решаться следующие задачи:

1) восстановление стертых файлов и стертых записей в базах данных, уточнение времени уничтожения, внесения изменений, копирования и модификации компьютерной информации;
2) установление времени ввода в компьютер определенных файлов, записей в базы данных;
3) расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;
4) выяснение каналов утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных;
5) выяснение технического состояния и исправности средств компьютерной техники.

Наряду с этими основными задачами при проведении программно-технической экспертизы могут быть решены и некоторые задачи вспомогательного характера, а именно:

1) оценка стоимости компьютерной техники, периферийных устройств, магнитных носителей, программных продуктов, а также проверка контрактов на их поставку;
2) установление уровня профессиональной подготовки отдельных лиц в области программирования и работы со средствами компьютерной техники;
3) перевод документов технического содержания. В связи с тем, что при осмотре ЭВМ и носителей информации производится изъятие различных документов, в ходе расследования может возникнуть необходимость в назначении криминалистической экспертизы для исследования документов. Дактилоскопическая экспертиза позволит выявить на документах, частях ЭВМ и машинных носителях следы пальцев рук причастных к делу лиц.

Оценка проведенных экспертиз компьютерных систем, компьютерных программ и информации, а также тактика их использования в качестве доказательств по делу, в сущности, не отличаются от оценки и использования заключений экспертиз традиционных видов [108, 22; 178; 179, 21].

На основе анализа изложенного, представляется возможным сделать следующие выводы:

- судебно-технологическая (компьютерная) экспертиза — представляет собой новый вид судебный экспертизы, необходимость которой обуславливается широким внедрением компьютерной техники и технологий практически во все сферы человеческой деятельности;
- предметом судебной экспертизы средств компьютерной технологии являются обстоятельства дела, связанные с установлением: конструктивных особенностей и технического состояния компьютеров и периферийных устройств; информации, содержащейся в оперативной памяти

компьютера и на магнитных носителях; способов изменения компьютерных программ;

- объектами судебно-компьютерной (технологической) экспертизы могут являться: компьютеры в сборке и их системные блоки; компьютерные системы (компьютерные сети); периферийные устройства (дисплеи, принтеры, дисководы, модемы, клавиатуры, сканеры, манипуляторы, джойстики и так далее); коммуникационные устройства компьютеров и вычислительных систем; технические средства и магнитные носители информации (жесткие, флоппи-диски, оптические диски, ленты), множительная техника, средства спецтехники и связи; электронные записные книжки, пейджеры, иные носители текстовой или цифровой информации, техническая документация к ним; распечатки программных и текстовых файлов; словари поисковых признаковых систем, классификаторы; документы, изготовленные с использованием компьютерных систем и электронных средств передачи и копирования информации (факсы, ксерокопии и так далее); компьютерная информация (программы, тексты); программное обеспечение различных форм, типов, видов, функционального назначения и способов исполнения; документы (договоры на покупку, создание (передачу) научно-технической продукции; калькуляции стоимости этапов предпродажной подготовки компьютеров; сопроводительная документация к компьютерной, вычислительной технике; справочные данные; инструкции пользователя и другое); системные процессы обмена информацией и связи между элементами компьютерных систем; видео- и звукозаписи, визуальная и аудиоинформация, в том числе на лазерных дисках; материалы дела, относящиеся к предмету экспертных исследований;
- методами исследования являются: квалифицированное наблюдение, системный анализ, математическое моделирование, инструментальный анализ с применением ЭВМ, статистический и социальный эксперимент, метод экспертных оценок, специальные методы предметных наук;
- при разработке методик экспертного исследования средств компьютерной техники важно чтобы ее разработчики имели углубленные знания об архитектонических свойствах и особенностях компьютерной техники и ее средств. А для возможности установления различных аспектов (распознавания периода и времени нажатия на клавиши терминала, определения профессиональных навыков пользователя ЭВМ и так далее) необходимо, прежде всего, наличие специальных компьютерных программ, а также высококлассное оборудование и качественное оснащение помещений, в которых осуществляется производство судебной экспертизы;
- задачи, решаемые судебно-технологической (компьютерной) экспертизой, делятся на диагностические и идентификационные.

Диагностические задачи (или задачи общего системного анализа):

- диагностика и классификация систем (например, классификация компьютерной системы (принтера, факса, копира) по тексту, изготовленному с ее применением; отнесение информации к категории программного обеспечения ЭВМ);
- определение структуры и функций систем; определение элементов системы и ее границ;
- анализ системных норм; определение семантики и прагматики спорных текстов, работы неизвестных компьютерных систем, воздействия деятельности систем на окружающую микро- и макросреду;
- реконструкция и прогнозирование поведения систем;
- определение надежности и устойчивости компьютерных систем; отнесение конкретных программ к вредоносным;
- реконструкция ОМП методами математического анализа и компьютерного моделирования;
- криминалистическая диагностика роли и функционального назначения отдельных элементов компьютерной системы, диагностика межэлементных связей и отношений;
- криминалистическая диагностика системных процессов и поведения систем;

Идентификационные задачи:

- идентификация системы;
- идентификация автора машинного текста;
- системный анализ обстановки места происшествия (ОМП);
- диагностика интеллектуального взлома системы.

В соответствии с задачами исследования, судебно-компьютерную экспертизу можно разделить на два вида:

1) техническая экспертиза компьютеров и их комплектующих (конструкция компьютера, магнитных носителей, компьютерных сетей и их работа);
2) экспертиза программного обеспечения (исследование информации, хранящейся в компьютере и на магнитных носителях).

Учитывая специфичность исследования, для разрешения ряда вопросов не технического характера, возможно совмещение программно-технической экспертизы с другими.

Программно-технической экспертизой могут решаться следующие задачи:

1) восстановление стертых файлов и стертых записей в базах данных, уточнение времени уничтожения, внесения изменений, копирования и модификации компьютерной информации;
2) установление времени ввода в компьютер определенных файлов, записей в базы данных;
3) расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;
4) выяснение каналов утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных;

5) выяснение технического состояния и исправности средств компьютерной техники.

Наряду с основными задачами при проведении программно-технической экспертизы могут быть решены и задачи вспомогательного характера, а именно:

1) оценка стоимости компьютерной техники, периферийных устройств, магнитных носителей, программных продуктов, а также проверка контрактов на их поставку;
2) установление уровня профессиональной подготовки отдельных лиц в области программирования и работы со средствами компьютерной техники;
3) перевод документов технического содержания.

В завершении хотелось бы отметить, что в настоящее время программно-технические экспертизы и подобные исследования целесообразнее поручать группе специалистов в области компьютерных технологий, обладающих специальными системотехническими и программными познаниями, с целью разрешения большего объема поставленных следствием вопросов. Для единообразного оформления и способов изъятия компьютерной техники, а также в целях информирования следственного аппарата об объеме возможностей экспертов. В сфере компьютерных технологий, на наш взгляд, необходим общий документ (возможно инструкция), подготовленный экспертными отделами. С учетом развития возможностей экспертизы, а также на основе обязательного анализа практики изъятия, осмотра и исследования компьютерной техники и информации необходимо регулярное издание служебной литературы по означенным моментам и проведение занятий с сотрудниками следственных (а при необходимости и других) подразделений в целях повышения профессионального уровня.

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. Под перехватом сообщений, передаваемых по техническим и компьютерным каналам связи, следует понимать действия органа уголовного преследования, а также физических или юридических лиц по поручению органа уголовного преследования, направленные на копирование, блокирование, изъятие и уничтожение передаваемой информации, с целью получения доказательств по делу.

2. Перехват сообщений является самостоятельным следственным действием, поскольку имеет отличие от других следственных действий по своей цели, объекту, методу, условиям, задачам, срокам, порядку проведения.

Целью перехвата сообщений, передаваемых по техническим, в том числе, компьютерным каналам связи и снятие с компьютерных систем информации, является обнаружение информации, передаваемой по техническим, в том числе, и компьютерным каналам связи об обстоятельствах, подлежащих доказыванию по уголовному делу и использования ее при расследовании преступлений.

К задачам перехвата сообщений, передаваемых по техническим, в том числе компьютерным каналам связи и снятие с компьютерных систем информации относятся копирование, блокирование, изъятие, уничтожение информации и порядку его осуществления.

Объектом перехвата сообщений являются — компьютерная система, компьютерная сеть, технические каналы связи, исследование которых позволит органу уголовного преследования получить интересующую информацию.

К условиям производства перехвата сообщений относятся:

- специфика сообщений, которые планируется перехватить, должна быть четко обозначена в постановлении (входящие и (или) исходящие);
- разовый или продолжительный характер перехвата сообщений;
- время проведения перехвата сообщений, которое должно быть по возможности ограничено;
- необходимость продления первоначального срока перехвата сообщений, которое производится на основании нового постановления следователя, санкционированного прокурором;
- необходимость санкции прокурора, за исключением безотлагательных ситуаций (на основе оперативно-розыскной информации, заявления участников процесса);
- участие специалиста;
- решение вопроса о судьбе перехваченных сообщений.

Субъектами, имеющими право назначать перехват сообщений, являются прокурор, следователь, дознаватель.

В зависимости от вида системы (глобальная, локальная), в которую необходимо проникнуть и распределения подключенных к ней терминалов, может изменяться статус прокурора, санкционирующего данное действие.

Перехват сообщений, передаваемых с технических, в том числе, компьютерных каналов связи, осуществляется по юридическим (постановления) и фактическим (оперативно-розыскная информация, заявления участников уголовного процесса и другие доказательства, полученные по уголовному делу) основаниям.

Перехват сообщений, передаваемых по техническим, в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации может носить «продолжительный» и «разовый» характер.

«Продолжительный» вид перехвата сообщений устанавливается до двух месяцев — в пределах первоначального срока, установленного для производства предварительного следствия. Дальнейшее продление первоначального срока производства перехвата сообщений осуществляется в соответствии с положениями ст. 196 УПК РК «Срок предварительного следствия», определяющими основания и порядок продления сроков расследования уголовного дела. Обстоятельства, послужившие основанием для продления срока перехвата сообщений и ожидаемые результаты его производства, могут быть указаны в составляемом следователем постановлении о продлении сроков следствия, наряду с основными положениями, обусловливающими необходимость продления сроков расследования, либо в отдельном постановлении. Санкционирование данного решения производится прокурорами в соответствии с положениями ч. ч. 4, 5 ст. 196 УПК РК.

«Разовый» вид перехвата сообщений характеризуется возможностью уменьшения сроков его проведения и обусловливается следующими обстоятельствами:

- в случаях, когда следствие интересует возможность получения или отправления лицом с использованием компьютерной техники различных сообщений, перехват сообщений назначается с целью установления данного вопроса;
- в случаях, когда перехват сообщений производится до получения интересующей следствие информации и следствию известны сроки ее передачи (на основе заявлений участников уголовного процесса, оперативно-розыскной информации и другого).

При расследовании уголовного дела в форме дознания действуют установленные выше сроки, за исключением того, что «продолжительный» срок перехвата сообщений будет ограничиваться тридцатисуточным сроком в соответствии со ст. 285 УПК РК. Производство же перехвата сообщений в 10-дневный срок будет носить «разовый» характер и необходимость его назначения должна определяться указанными обстоятельствами.

Основными процессуальными способам обнаружения, изъятия информации передаваемой по техническим, в том числе компьютерным каналам связи являются: осмотр, выемка, розыск в компьютерных сетях, перехват сообщений.

При перехвате сообщений, передаваемых по техническим, в том числе компьютерным каналам связи и снятие с компьютерных систем информации используются специальные средства при получении, исследовании информации, осуществлению взлома при наличии пароля на сообщение, дополнительные средства фиксации.

Перехват сообщений, передаваемых по техническим, в том числе компьютерным каналам связи и снятие с компьютерных систем, реализуется в следующем порядке:

- определение цели и оснований для производства перехвата сообщений;
- определение объекта и системы, в которой планируется производство перехвата;
- определение участников проводимого действия;
- определение органа, осуществляющего перехват;
- определение срока и порядка передачи перехваченной информации;
- вынесение постановления;
- санкционирование постановления прокурором;
- получение перехваченной информации от исполняющего органа;
- осмотр полученной информации и принятие решения о ее дальнейшей судьбе.

3. В сферу уголовного судопроизводства вошли новые по природе источники доказательственной информации:

- компьютер (персональный компьютер, ЭВМ) — комплекс электронных устройств, позволяющих производить предписанные программой и пользователем операции (сбор, накопление, хранение, обработку, выдачу информации, включая передачу ее по телекоммуникационным сетям и тому подобные) над символьной и образной информацией и через установленные каналы выходить в информационно-вычислительную сеть, а также к источникам массовой информации;
- компьютерная система (вычислительная система, локальная система, автоматизированная система, система ЭВМ) — любая система, в состав которой входит компьютер, предназначенный для управления этой системой либо для принятия решений, а также включающая в себя аппаратное (совокупность технических устройств и приборов, используемых в работе с компьютером) и программное (совокупное название программных и информационных ресурсов, используемых в работе с компьютером) обеспечение и персонал, действующих совместно;
- компьютерная сеть (сеть ЭВМ) — единый комплекс, в которой ЭВМ взаимодействуют друг с другом, передают и получают информацию посредством каналов связи. Существует два вида состава компьютерной сети:

а) локальная сеть — сеть, компьютеры которой сосредоточены в пределах одного или нескольких предприятий или учреждений на небольшом расстоянии друг от друга (обычно до 10-20 км), а зачастую в одном здании;

б) глобальная сеть — сеть, компьютеры которой находятся на большом расстоянии друг от друга (от 10-20 до десятков тысяч км), имеющая систему обмена данных, позволяющую осуществить доступ к данным из ЭВМ на другом континенте, состоящая из локальных сетей, а также многотерминальных систем, систем виртуального доступа и другого.

Канал связи — часть сети, связывающая между собой каждую пару ее оконечных терминалов и состоящая из технических средств передачи и приема данных, включая линию связи, а также средств программного обеспечения и протоколов. В зависимости от характера, принципа построения, назначения и использования, различают каналы проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной, аналоговой, цифровой, дуплексной (двухсторонней) связи и так далее.

Линия связи — физическая среда, по которой осуществляется передача данных между терминалами сети. В зависимости от ее характера, принципа построения, назначения и использования различают линии проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной и других видов связи.

Сети электросвязи — 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.

4. Одним из способов обнаружения, изъятия информации из технических каналов связи может являться розыск в компьютерных сетях (или в среде для хранения компьютерных данных), который представляет собой систему процессуальных и оперативно-розыскных мероприятий, направленных на обнаружение, закрепление и изъятие в компьютерных сетях следов преступлений, а также иной компьютерной информации, имеющей значение для расследования и разрешения дела по существу, которая после надлежащего документирования может стать доказательством при расследовании преступлений. Необходимо законодательно определить и наделить полномочиями по розыску в компьютерных сетях (или в среде для хранения компьютерных данных) специальные правоохранительные органы или службы. Необходимо ввести в законодательство РК нормы, согласно которым:

– телекоммуникационные службы и Internet-провайдеры обязаны по запросу правомочных правительственных учреждений и органов принять все необходимые меры к сохранению данных или других свидетельств, имеющихся в их распоряжении, до издания соответствующего решения, на основе которого эти данные изымаются в распоряжение органов правосудия;

– компетентные органы вправе получить запрашиваемые данные в течение определяемого законодателем срока их хранения.

5. Компьютерная информация может иметь типичные и факультативные свойства, которые могут быть использованы для идентификации файла и находящейся в нем информации, что имеет важное значение при расследовании компьютерных преступлений.

К типичным свойствам относятся:

– наименование файла (включая его местоположение на логическом диске);
– размер файла;
– время создания, модификации;
– системные атрибуты («системный», «только для чтения» и другие);
– тип информации, хранящейся в файле (текстовая, графическая и так далее);
– машинный носитель, его тип, номер, метка и другое.

К факультативным свойствам относятся:

– программные средства, с использованием которых был создан или модифицирован файл (использование специальных символов, выделений, отметок в коде программы или документе, указателей на версию, серийный номер программного продукта, зарегистрированный пользователь программного продукта и другое);
– автор, создавший или модифицирующий файл (программу в целом);
– группа файлов (программные средства, группы документов), куда включен файл (в качестве отдельного документа или части программного кода);
– ключевые слова, заметки автора или редактора и тому подобное.

Приведенные выше свойства файлов, при отражении их в протоколах следственных действий, позволят удостоверить относимость, допустимость и достоверность полученной информации, при ее дальнейшем использовании в качестве доказательства при расследовании уголовных дел.

6. Перехват сообщений является одним из действий, в ходе которого становится известной информация об исключительно частной жизни лица. В связи с чем, сотрудники полиции, осуществляющие операции над получаемой информацией (в том числе и личного характера), должны руководствоваться в своей деятельности принципами уважения и защиты человеческого достоинства по отношению ко всем лицам. И обязаны, в соответствии со ст. ст. 53, 205 УПК РК, предупредить участников проводимого действия о недопустимости разглашения ставших им известными сведений и ответственности за их разглашение без согласия следователя по ст. 355 УК РК.

7. Правильное осуществление получения и использования информации с технических каналов связи и получение информации из компьютерных систем зависит от однозначного понимания терминов, используемых при документировании и расследовании преступлений. На основании теоретического, норма-

тивного исследования предлагается следующая трактовка основных дефиниций:

Компьютерная информация — информация, зафиксированная на машинном, магнитном носителе, представленная в форме набора состояний элементов ЭВМ, иных электронных средств обработки, хранения и передачи информации. Компьютерная информация может являться подлинником или копией. Подлинник — первая по времени запись на машинном носителе; копия — более поздняя запись, аутентичная по содержанию, переписанная с подлинника. Изменение подлинника может производить только лицо или организация — создатель документа; изменения в копии вносятся на основании извещения об изменениях.

Машинограмма — документ на бумажном носителе, созданный средствами вычислительной техники в письменной форме и оформленный в установленном порядке. На машинограммах, представляющих особо важную информацию, подпись удостоверяется печатью организации — создателя документа.

Электронный документ (машиночитаемый документ) — совокупность данных, оформленная в установленном порядке и представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, зафиксированная на машиночитаемом носителе, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств и имеющая атрибуты идентификации документа. Электронный документ должен:

- создаваться, обрабатываться, храниться, передаваться и приниматься с помощью программных и технических средств;
- содержать реквизиты, позволяющие подтвердить его подлинность и целостность;
- быть отображенным (воспроизведенным) в форме, понятной для восприятия человеком.

Электронный документ может объединять в себе несколько пересылаемых файлов. Каждый файл, входящий в электронный документ, может иметь одну или несколько электронных подписей и не обязательно отправителя. Данный вид электронного документа должен включать в себя файл-реестр с перечнем файлов, вошедших в документ. В реестре для каждого файла указывается его имя и информация о том, является ли он подписанным или нет. Приложением к такому электронному документу будет являться протокол, содержащий указание о том, кому он предназначен и, возможно, некоторую дополнительную служебную информацию. Любой электронный документ или компьютерная информация могут быть зашифрованы.

Материальный носитель — обобщающее наименование материала, на который можно записывать данные. Носители подразделяются на: машиночитаемый носитель — пригодный для непосредственной записи и считывания данных техническими средствами (ЭВМ) — магнитные и оптические диски, дискеты и тому подобное; человекочитаемый (твердый) носитель — пригодный или

используемый для записи данных, непосредственно считываемых человеком — бумага, фото-, кино- и фонодокументы и другое.

Личная информация (информация персонального характера) — сведения о политических взглядах, философских, религиозных и других убеждениях, о принадлежности к политическим партиям, общественным движениям и ассоциациям, личной жизни, включая интимные ее стороны и сексуальное поведение, сведения о национальности, о состоянии физического и психического здоровья, о потреблении алкоголя и иных наркотических и токсических веществ, вкладах в банке, других видах собственности, а также сведения о погашенной судимости; сведения, данные о гражданах и организациях, затрагивающих их интересы и запрещенные для распространения без их согласия.

Документ — материальный носитель, на котором условными знаками (буквами, цифрами и другими) зафиксирована информация о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека, в том числе и информация, имеющая правовое значение и отражающая ход и результаты деятельности участников уголовного судопроизводства, с реквизитами, позволяющими ее идентифицировать.

Процессуальные документы — документы, содержащие фактические данные, полученные в ходе следственных и судебных действий, оформленные и удостоверенные органами уголовного преследования в установленном Уголовно-процессуальным кодексом порядке, и имеющие в соответствии с действующим законодательством правовое значение.

Иные документы — разного рода документы, изготовленные как в ходе процессуальной деятельности, так и вне ее, но используемые в процессе как источники доказательств: материалы доследственной проверки; *официальные и частные* документы, полученные, истребованные или представленные в порядке, предусмотренном ст. 125 УПК РК.

Официальные документы — документы, электронные документы, созданные физическим или юридическим лицом, оформленные и удостоверенные в установленном порядке, имеющие в соответствии с действующим законодательством правовое значение. Официальные документы, исходящие или выдаваемые организациями, предприятиями, учреждениями любой юридической природы, характеризуются наличием в них реквизитов. Реквизитами являются: бланк документа его форма, цвет, размер, наличие защитных средств, оттисков печатей и штампов, фотокарточки, подписи должностных лиц.

Частные документы — документы, созданные физическим лицом, не имеющие какой-либо обязательной нормы и реквизитов (частные записки, личные письма и другие).

8. Анализ практики реализации норм о получении информации с технических каналов связи и компьютерных систем, а также теоретическое и правовое исследование позволили диссертанту разработать рекомендации по совершенствованию законодательной регламентации применения данного вида следственного действия. Предлагается внести изменения в понятие перехвата сооб-

щений, законодательно закрепить основание, порядок, сроки проведения. В частности, предлагается:

Статью 236 УПК РК изложить в следующей редакции:

«1. Перехват сообщений, передаваемых по техническим, в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации, относящейся к расследуемому делу, производятся на основании постановления следователя, санкционированного прокурором с целью получения информации об обстоятельствах, имеющих значение для дела.

2. Постановление следователя о производстве перехвата сообщений должно содержать номер уголовного дела и основания, по которым должно производиться данное действие, данные о лице, чьи сообщения подлежат перехвату. В постановлении должны быть указаны сроки передачи относимой к делу информации, вид канала связи, либо компьютерной системы, которая должна контролироваться.

3. Перехват сообщений и снятие с компьютерных систем информации производится на основании фактических данных, дающих основание полагать, что в информации, поступающей и отправляемой подозреваемым, обвиняемым могут содержаться сведения, имеющие значение для дела, а также для своевременного предотвращения готовящихся преступных деяний.

4. Перехват сообщений потерпевшего, свидетеля и других участников уголовного процесса допускается при наличии угрозы совершения насилия, вымогательства либо других противоправных действий в отношении этих лиц на основании соответствующего заявления или с их согласия на перехват сообщений.

5. Перехват сообщений свидетелей, потерпевших, других участников уголовного процесса допускается без их согласия при наличии информации о том, что они совершают действия по укрывательству преступления, орудий и средств совершения преступления, предметов, добытых преступным путем, препятствуют установлению истины по делу, обмениваются информацией с подозреваемым, обвиняемым.

6. Перехват сообщений, передаваемых по техническим, в том числе и компьютерным каналам связи, и снятие с компьютерных систем информации устанавливается на срок до двух месяцев. Дальнейшее продление срока производится в соответствии с положениями ч. ч. 4, 5, 6, 7 ст. 196 УПК РК.

7. О приостановление перехвата сообщений указывается в постановлении о приостановлении предварительного следствия или в отдельном постановлении «о приостановлении производства перехвата сообщений» вынесенном следователем, дознавателем, прокурором.

8. Производство перехвата сообщений прекращается по постановлению следователя, дознавателя, прокурора, если необходимость в данной мере отпадает, но не позднее окончания расследования по данному уголовному делу.

9. Возобновление производства перехвата сообщений производится на основании положений ч. ч. 1, 2 ст. 268 УПК РК или наряду с возобновлением предварительного следствия. В постановлении должно быть указано — сохраняется

ли прежний режим перехвата сообщений или изменяется. Установленные изменения указываются в выносимом постановлении.

10. Постановление следователя, санкционированное прокурором, направляется для исполнения органу, осуществляющему ОРД, или администрации телефонного узла, телефонной станции, организациям и учреждениям, осуществляющих предоставление услуг по работе в компьютерных сетях.

11. Санкция на перехват сообщений абонентов в пределах населенного пункта дается районным, городским прокурором или их заместителями; в пределах области или территории Республики Казахстан — прокурорами областей и приравненных к ним прокурорами.

12. Сообщения и компьютерная информация, полученные в результате перехвата, фиксируются специалистом на соответствующем носителе и передаются следователю в опечатанном виде с указанием даты, времени перехвата и краткой характеристики использованных при этом технических средств.

13. Полученная при перехвате сообщений информация копируется на машинный носитель, после чего, по решению органа уголовного преследования может быть направлена адресату, блокирована, изъята или уничтожена. Операции, проводимые над информацией, отражаются в протоколе осмотра предметов и документов, согласно требованиям, установленными ст. ст. 221, 222, 223, 227 УПК РК».

9. Предлагается дополнить УПК РК новой статьей — ст. 217-1 «Допрос специалиста», изложив ее в следующей редакции:

«Если необходимо уточнить примененные специалистом методы и термины, а также выяснить ряд других вопросов, связанных с участием специалиста при проведенном следственном действии, следователь (дознаватель) вправе допросить специалиста.

Перед началом допроса специалисту разъясняются его права и обязанности, и он предупреждается об ответственности за заведомо ложные показания по ст. 352 УК РК.

Протокол допроса специалиста составляется с соблюдением правил, предусмотренных ст. 218 УПК РК.

В случае необходимости получения сведений консультативного, справочного характера, следователь (дознаватель) может пригласить специалиста для их получения. Предоставление сведений, носящих специальный характер, оформляется в виде справки, подписанной специалистом. К справке могут быть приложены схемы, таблицы, графики и другие материалы. Приложение подписывается специалистом».

10. Дополнить УПК РК ст. 251-1: «Исследование специалиста», изложив ее в следующей редакции:

«Исследование, проводимое специалистом, производится в случаях, когда обстоятельства, имеющие значение для дела, могут быть получены на основе специальных знаний до производства экспертизы. Полученные результаты, не освобождают лицо, ведущее уголовный процесс, от необходимости в соответствующих случаях назначить экспертизу.

Ход и результаты исследования отражаются в протоколе исследования, приобщаемом в качестве приложения к протоколу следственного действия (ч. 8 ст. 203 УПК РК).

Протокол исследования — письменный документ, в котором отражены выводы по вопросам, поставленным перед специалистом, основанные на результатах проведенного с использованием специальных знаний исследования. В протоколе должно быть указаны: когда, где, кем, проведено исследование, какие материалы уголовного дела им исследованы; в рамках какого следственного или судебного действия он участвовал; какие объекты были подвергнуты исследованию; какие исследования произведены; какие методы и средства применены и в каком виде они надежны; если при исследовании специалист установит обстоятельства, имеющие значение для дела, по поводу которых ему не было изложено в задании, он вправе указать их в своем документе.

К протоколу исследования прилагаются исследованные объекты, а также фототаблицы, графики, модели, слепки, оттиски, схемы и другие материалы, подтверждающие выводы специалиста. Данный документ подписывается специалистом и лицами, присутствующими при исследовании».

11. Предлагается исключить п. 5 ч. 1 ст. 96 УПК РК «Если он участвовал в деле в качестве специалиста, за исключением случаев участия в соответствии со ст. 224 настоящего кодекса врача-специалиста в области судебной медицины в осмотре трупа человека».

12. Дополнить ч. 1 ст. 96 УПК РК «Отвод эксперта», пунктами:

«6) если он признан в установленном законом порядке ограниченно дееспособными и недееспособными;

7) если он ранее судим;

8) если он уволен по отрицательным мотивам с должности, связанной с осуществлением судебно-экспертной деятельности».

13. Анализ практики, а также теоретическое и нормативное исследование позволили сделать рекомендации по совершенствованию законодательной регламентации организации производства экспертизы. Так, в частности, предлагается:

Изменить п. 3 ч. 1 ст. 243 УПК РК «Лица, которым, может быть поручено производство судебной экспертизы» и изложить в следующей редакции:

«в разовом порядке в случаях:

- назначения экспертизы, не предусмотренной определенным законодательством перечнем видов экспертиз;
- привлечения в качестве эксперта специалиста иностранного государства в области судебной экспертизы, в соответствии со ст. 27 Закона РК «О судебной экспертизе»;
- удовлетворения отводов всем экспертам соответствующей специальности, являющимся сотрудниками органов судебной экспертизы, а также осуществляющим судебно-экспертную деятельность на основании лицензии (на производство экспертизы), либо мотивированного отстранения от производства экспертизы этих лиц и соответствующего органа».

Дополнить ч. 1 ст. 352 УК РК после слов «1. Заведомо ложные показания, свидетеля, потерпевшего» словом «специалиста», и далее по тексту.

14. Процессуальным способом обнаружения, исследования и оценки компьютерной информации выступают следующие виды судебно-технологической (компьютерной) экспертизы:

- техническая экспертиза компьютеров и их комплектующих (конструкция компьютера, магнитных носителей, компьютерных сетей и их работа);
- экспертиза программного обеспечения (исследование информации, хранящейся в компьютере и на магнитных носителях)

Предметом судебной экспертизы средств компьютерной технологии являются обстоятельства дела, связанные с установлением:

- конструктивных особенностей и технического состояния компьютеров и периферийных устройств;
- информации, содержащейся в оперативной памяти компьютера и на магнитных носителях;
- способов изменения компьютерных программ.

Объектами судебно-компьютерной (технологической) экспертизы являются:

- компьютеры в сборке и их системные блоки;
- компьютерные системы (компьютерные сети);
- периферийные устройства (дисплеи, принтеры, дисководы, модемы, клавиатуры, сканеры, манипуляторы, джойстики и так далее);
- коммуникационные устройства компьютеров и вычислительных систем;
- технические средства и магнитные носители информации (жесткие, флоппи-диски, оптические диски, ленты), множительная техника, средства спецтехники и связи;
- электронные записные книжки, пейджеры, иные носители текстовой или цифровой информации, техническая документация к ним;
- распечатки программных и текстовых файлов;
- словари поисковых признаковых систем, классификаторы;
- документы, изготовленные с использованием компьютерных систем и электронных средств передачи и копирования информации (факсы, ксерокопии и так далее);
- компьютерная информация (программы, тексты);
- программное обеспечение различных форм, типов, видов, функционального назначения и способов исполнения;
- документы (договоры на покупку, создание (передачу) научно-технической продукции; калькуляции стоимости этапов предпродажной подготовки компьютеров; сопроводительная документация к компьютерной, вычислительной технике; справочные данные; инструкции пользователя и другое);

- системные процессы обмена информацией и связи между элементами компьютерных систем;
- видео- и звукозаписи, визуальная и аудиоинформация, в том числе на лазерных дисках;
- материалы дела, относящиеся к предмету экспертных исследований.

Основными методами исследования таких объектов являются квалифицированное наблюдение, системный анализ, математическое моделирование, инструментальный анализ с применением ЭВМ, статистический и социальный эксперимент, метод экспертных оценок, специальные методы предметных наук.

При производстве судебно-компьютерной (технологической) экспертизы могут решаться диагностические и идентификационные задачи.

Теоретические положения и практические рекомендации работы используются в практической деятельности органов предварительного следствия и дознания (см. Приложение Ж), прокуратуры, военного (см. Приложение И) и городского (см. Приложение К) судов, а также внедрены в учебный процесс по дисциплинам «Предварительное следствие РК», «Дознание и предварительное следствие в РК» в Карагандинском юридическом институте МВД РК имени Баримбека Бейсенова (см. Приложение Л) и «Уголовно-процессуальное право», «Криминалистика» в КазГЮУ г. Астаны (см. Приложение М).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 ***Назарбаев Н. А.*** К свободному, эффективному и безопасному обществу: Послание Президента страны народу Казахстана // Юридическая газета. 2000. 25 окт.

2 ***Назарбаев Н. А.*** Послание Президента страны народу Казахстана: «Казахстан-2030». — Астана, 2000. — 108 с.

3 Программа действий Правительства, утвержденная Указом Президента РК, «О мерах по реализации Стратегии развития Казахстана до 2030 года. Казахстан-2030» от 28 января 1998 г. № 3834.

4 ***Ожегов С. И.*** Словарь русского языка. — М., 1972. — 900 с.

5 Юридический энциклопедический словарь / Под ред. А. Я. Сухарева. — М., 1987. — 82 с.

6 ***Афанасьев В. Г.*** Социальная информация и управление обществом. — М., 1975. — 408 с.

7 ***Берг А. И.*** Информация и управление. — М., 1966. — 64 с.

8 ***Тюхтин В.*** Теория отражения в свете современной науки. — М., 1971. — 48 с.

9 ***Урсул А.*** Природа информации. Философский очерк. — М., 1968. — 288 с.

10 ***Павлов Т. Д.*** Информация, отражение, творчество. — М., 1966. — 149 с.

11 Словарь иностранных слов. — М., 1982. — 607 с.

12 Ленинская теория отражения и современная наука.— М., 1973. Т. 1 — 726 с.

13 ***Мамиконов А. Г.*** Управление и информация. — М., 1975. — 184 с.

14 ***Черри Д.*** Человек и информация. — М., 1972. — 145 с.

15 ***Овчинский С. С.*** Оперативно-розыскная информация. Теоретические основы информационно-прогностического обеспечения оперативно-розыскной и профилактической деятельности ОВД по борьбе с организованной преступностью. — М., 2000. — 367 с.

16 ***Эшби У. Р.*** Система и информация // Вопросы философии. — 1964. — № 3. — С. 22-27.

17 ***Урсул А. Д.*** Отражение и информация. — М., 1973. — 231 с.

18 ***Ларин А. М.*** От следственной версии к истине. — М., 1976. — 200 с.

19 ***Гусев Л. Н.*** Об основах уголовного судопроизводства СССР и союзных республик. — М., 1959. — 79 с.

20 ***Каз Ц.М.*** Доказательства в советском уголовном процессе. — Саратов, 1960. — 76 с.

21 ***Рахунов Р. Д.*** Некоторые вопросы доказательственного права в свете основ уголовного судопроизводства // Важный этап в развитии советского права: Сб. тр. — М.: Труды ВИЮН, 1960. — С. 80-83.

22 ***Арсеньев В. Д.*** Вопросы общей теории судебных доказательств. — М., 1964. — 179 с.

23 ***Карнеева Л. Р.*** Развитие основных понятий теории доказательств в советском уголовном процессе // Социалистическая законность. — 1978. — № 2. — С. 28-31.

24 ***Шейфер С. А.*** Сущность и способы собирания доказательств в советском уголовном процессе. — М., 1973. — 130 с.

25 ***Алексеев Н. С., Даев В. Г., Кокорев Л. Д.*** Очерк развития науки советского уголовного процесса. — Воронеж, 1980. — 147 с.

26 ***Василенко В. П., Трофимов А. Т.*** О понятии исследования доказательственной информации // Труды ВСШ МВД СССР. — Волгоград, 1976. Вып. 12. — С. 29-40.

27 ***Тетенькин Б. А.*** Проверка доказательств в структуре уголовно-процессуального доказывания: Автореф. … канд. юрид. наук. — М., 1983. — 21 с.

28 ***Черданцев А. Ф.*** Толкование советского права. — М., 1979. — 166 с.

29 Словарь современного русского литературного языка. — М.-Л., 1964. Т. 16. — 1215 с.

30 Комментарий к Закону «Об оперативно-розыскной деятельности» / Отв. ред. А. Ю. Шумилов. — М., 1997. — 130 с.

31 ***Лукашов В. А.*** О некоторых морально-этических аспектах оперативно-розыскной деятельности // Законность, оперативно-розыскная деятельность и уголовный процесс. — СПб., 1998. — С. 6-9.

32 Инструкции «О порядке изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, документов по уголовным, гражданским делам и делам об административных правонарушениях судом, органами прокуратуры, предварительного следствия, дознания, судебной экспертизы» утверждена приказами: Генерального прокурора РК № 1034 ЦА от 1 декабря 1998 г.; Председателя КНБ РК № 73 от 8 декабря 1998 г.; Министра финансов РК № 598 от 22 декабря 1998 г.; Министром юстиции РК № 121 от 12 ноября 1998 г.; Министром МВД РК № 429 от 2 декабря 1998 г.; исполняющим обязанности Министра госдоходов РК № 11 от 28 декабря 1998 г.

33 ***Батурин Ю. М., Жодзишский А. М.*** Компьютерная преступность и компьютерная безопасность. — М., 1991. — 158 с.

34 ***Шумилов А .Ю.*** Закон и оперативно-розыскная деятельность (толковый словарь понятий и терминов, используемых в законодательстве в области ОРД). — М., 1996. — 77 с.

35 ***Бедняков Д. И.*** Непроцессуальная информация и расследование преступлений. — М., 1991. — 208 с.

36 ***Кондаков Н. И.*** Логический словарь-справочник. — М., 1975. — 720 с.; ***Брушлинский А. В.*** Деятельность, действие и психическое как процессы // Вопросы психологии. — 1984. — № 5. — С. 22-25.

37 Философский словарь / Под ред. И. Т. Фролова. — М., 1980. — 444 с.

38 Гражданский Кодекс РФ (принят 21 октября 1994 г.). — М., 1997. Ч. 1. — 448 с.

39 Словарь основных уголовно-процессуальных понятий и терминов / Под ред. Б. Х. Толеубековой. — Караганда, 1992. — 123 с.

40 Федеральный Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. // Юридический вестник — 1996. — № 4. — С. 15-23.

41 Федеральный закон РФ «Об участии в международном информационном обмене» от 4 июля 1996 г. // Юридическая газета. 1996. 2 авг.

42 Краткий словарь современных понятий и терминов / Сост. А. Т. Трофимов, Н. И. Кондаков. — М., 1995. — 125 с.

43 Закон Республики Казахстан «О национальном архивном фонде и архивах» от 22 декабря 1998 г. // Ведомости Парламента РК. — 1998. — № 24 — Ст. 435.

44 ***Воройский Ф. С.*** Систематизированный толковый словарь по информатике. — М., 1998. — 250 с.

45 Уголовный процесс: Учебн. / Под ред. И. Л. Петрухина. — М., 2001. — 520 с.

46 ***Столяров Ю. Н.*** Документный ресурс: Учеб. пос. — М., 2001. — 152 с.

47 Приказ Государственного комитета СССР по делам изобретений и открытий «Об утверждении Положения о всесоюзной магнитно-ленточной службе патентной информации» от 29 декабря 1980 г. № 158.

48 Временные общеотраслевые руководящие указания «О придании юридическим документам, создаваемым средствами вычислительной техники» от 20 апреля 1981 г. — М., 1981. — 19 с.

49 Документ в информационном обществе: Сб. мат-лов VI международной научно-практической конференции. — М., 1999. — 120 с.

50 Национальный стандарт по управлению документами. — Австралия, 1996. — 247 с.

51 ***Сергеев К.*** Компьютерная экзотика, или электронный договор // Law and Internet. — М., 2001. — С. 8-12.

52 Проект закона РФ «Об электронно-цифровой подписи» в редакции от 15 мая 2000 г. — М., 2000. — 15 с.

53 ***Соловьев Н. Н.*** Электронные документы. Какие они? // Мир ПК. — 2002. — № 3. — С. 55-56.

54 ***Артюхов С.*** Электронно-цифровой подписи — законную силу // Мир ПК. — 2002. — № 4. — С. 97-99.

55 Закон Туркменистана «Об электронном документе» от 19 декабря 2000 г.

56 Постановление Кабинета Министров Республики Казахстан «Об утверждении Основных правил документирования и управления документацией в объединениях (предприятиях), учреждениях и организациях всех организационно-правовых форм Республики Казахстан» от 30 июня 1992 г. № 562.

57 Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. № 370-II // Казахстанская правда. 2003. 10 янв.

58 ***Треушников М. К.*** Судебные доказательства. — М., 1997. — 175 с.

59 ***Молчанов В. В.*** Доказывание и доказательства (Глава 5) // Арбитражный процесс. — М., 1995. — С. 249-340.

60 Теория доказательств в советском уголовном процессе. — М., 1973. — 735 с.

61 Приказ МВД Республики Казахстан «О повышении эффективности применения научно-технических методов и средств в борьбе с преступностью» от 31 мая 1993 г. № 210.

62 ***Треушников М. К.*** Доказательства (глава 6) // Комментарий к Гражданскому процессуальному кодексу РСФСР. — М., 1997. — С. 340-448.

63 ***Калиновский К. Б., Маркелова Т. Ю.*** Доказательственное значение «электронной» информации в Российском уголовном процессе // Российский следователь. — 2001. — № 6. — С. 18-19.

64 ***Толеубекова Б. Х.*** Компьютерная преступность: уголовно-правовые и процессуальные аспекты: Учеб. пос. — Караганда, 1991. — 82 с.

65 ***Крылов В. Б.*** Информационные компьютерные преступления. — М., 1997. — 285 с.

66 ***Симонович С., Евсеев Г.*** Практическая информатика: Учеб. пос. — М., 2000. — 464 с.

67 Современный словарь иностранных слов. — М., 1993. — 562 с.

68 ***Фигурнов В. Э.*** IBM PC для пользователя. — М., 1994. — 250 с.

69 Архив суда г. Петропавловск. 1998 г. Уголовное дело № 980710.

70 ***Акчурин А. Г., Акчурин А. А.*** Многофакторный анализ компьютерных преступлений. // Казахстан-2030. Проблемы совершенствования деятельности правоохранительных органов. — Алматы, 1999. — С. 386-387.

71 ***Возгрин И. А.*** Общие положения методики расследования отдельных видов преступлений. — Л., 1976. — 165 с.

72 ***Белкин Р. С.*** Курс советской криминалистики. Криминалистические средства, приемы и рекомендации. — М., 1979. Т. 3. — 407 с.

73 ***Васильев А. Н., Яблоков Н. П.*** Предмет, система и теоретические основы криминалистики. — М., 1984. — 143 с.

74 ***Белкин Р. С.*** Собирание, исследование и оценка доказательств. — М., 1986. — 295 с.

75 ***Кузьмин А. П.*** Использование ПЭВМ в расследовании преступлений: Автореф. дис. … канд. юрид. наук. — М., 1994. — 25 с.

76 Закон Республики Казахстан «О связи» от 13 мая 1999 г. // Казахстанская правда. 1999. 21 мая.

77 Конституция Республики Казахстан от 30 августа 1995 г. (с изменениями и дополнениями от 7 октября 1998 г.). — Алматы, 2002. — 40 с.

78 Закон Республики Казахстан «Об оперативно-розыскной деятельности» от 12 августа 1995 г. (с изменениями от 10 ноября 2001 г.) // Правоохранительные органы: Сб. законодательных актов. — Алматы, 2002. — С. 118-129.

79 ***Нургалиев Б. М., Арыстанбеков М. А.*** Наложение ареста на почтово-телеграфную корреспонденцию. Перехват сообщений. Прослушивание и запись переговоров // Криминалистическая тактика. — Караганда, 1999. — С. 174-186.

80 Словарь основных уголовно-процессуальных понятий терминов / Сост. А. М. Баранов, П. Г. Марцифин. — Омск, 1997. — 40 с.

81 Расследование преступлений повышенной общественной опасности: Пособие для следователя / Под ред. Н. А. Селиванова. — М., 1999. — 354 с.

82 ***Гульбин Ю.*** Преступления в сфере компьютерной информации // Российская юстиция. — 1997. — № 10. — С. 31-33.

83 Архив суда г. Алматы. Уголовное дело № 1252251203.

84 Законодательство зарубежных стран. Обзорная информация. — М., 1982. — 118 с.

85 Трактовка поправки IV к Конституции США, разработанная Верховным судом США в 1964-1965 гг. // Законодательство зарубежных стран. Обзорная информация. — М., 1971. — С. 19-21.

86 Закон «О контроле над преступностью и обеспечением безопасности на улицах». Принят Конгрессом США 19 июня 1968 г. // Законодательство зарубежных стран. Обзорная информация. — М., 1982. — С. 25-50.

87 ***Аксель Хорн и Ульф Мюллер.*** Выдержки из полного отчета отдела Европейского парламента по оценке научно-технологических разработок «Оценка технологий политического контроля» от 4 февраля 1998 г.

88 Рекомендации по применению средств видео-, звукозаписи, кинофотоаппаратуры, телефонной связи и использовании полученных результатов при предотвращении, раскрытии и расследовании преступлений // Прокуратура СССР. — М., 1990. — С. 25-28.

89 Архив ДКНБ РК г. Актюбинск. Уголовное дело № 216001.

90 ***Капсалямов К. Ж.*** Уголовное преследование и способы собирания доказательств: Учеб. пос. — Астана, 2001. — 98 с.

91 ***Чувилев А. Н.*** Процессуальные основания и порядок прослушивания и звукозаписи телефонных и иных переговоров в уголовном судопроизводстве. — М., 1999. — 124 с.

92 УПК Федеративной Республики Германия (§ 98). — М., 1954. — 128 с.

93 Федеральный Закон Российской Федерации «Об оперативно-розыскной деятельности в РФ» от 18 мая 1993 г.

94 О последних изменениях оперативно-розыскного и уголовно-процессуального законодательства, касающихся контроля и записи телефонных и иных переговоров // Российский следователь. — 2002. — № 5. — С. 21-22.

95 Примерные образцы уголовно-процессуальных актов досудебного производства. — Астана, 2000. — 206 с.

96 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. // Сборник кодексов РФ. — М., 2002. — С. 624 с.

97 Комментарий к уголовно-процессуальному кодексу Казахской ССР по состоянию на 15 мая 1995 г. — Алматы, 1995. — 646 с.

98 ***Симоров Д. Н.*** О последних изменениях оперативно-розыскного и уголовно-процессуального законодательства, касающихся контроля и записи телефонных и иных переговоров // Российский следователь. —2002. — № 5. — С. 19-21.

99 ***Мещеряков В. А.*** Преступления в сфере компьютерной информации: правовой и криминалистический анализ. — Воронеж, 2001. — 86 с.

100 ***Вихорев С. В.*** Что есть что в информационном праве // Filosof. — М., 2000. — С. 8-17; ***Ефремов А. А.*** Информация как объект гражданских прав // Filosof. — М., 2001. С. 10-22.

101 ***Волеводз А. Г.*** Следы преступлений, совершенных в компьютерных сетях // Российский следователь. — 2002. — № 1. — С. 18-20.

102 «Federal Criminal Code and Rules» Title 18. / Crime and Criminal Procedure (amendmenlieceivedio February 15, 1999). // West Group. St. Paul. — Minn, 1999. — P. 897-898.

103 Стив Басс // Мир ПК. — 2002. — № 4. — С. 94-95.

104 ***Чуркин А. В.*** Проникновение следователя в жилище при помощи компьютера: (точка зрения) // Российский следователь. — 1999. — № 4. — С. 44-45.

105 ***Арсеньев В. Д.*** Основы теории доказательств в советском уголовном процессе. — Иркутск, 1970. — 82 с.

106 ***Горский Г. Ф., Кокорев Л. Д., Элькинд П. М.*** Проблемы доказательств в советском уголовном процессе. — Воронеж, 1978. — 304 с.

107 Архив суда г. Кокшетау. 2001. Уголовное дело № 420081201.

108 Расследование преступлений в сфере компьютерной информации: Метод. реком. — М.: НИЛ № 4 ВНИИ МВД РФ, 1998. — 24 с.

109 ***Толеубекова Б. Х.*** Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники: Дис. … д-ра юрид. наук. — Алматы, 1998. — 380 с.

110 ***Назмышев Р. А.*** Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации: Дис. … канд. юрид. наук. — Костанай, 2000. — 130 с.

111 ***Рогозин В. Ю.*** Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Дис. … канд. юрид. наук. — Волгоград, 1998. — 281 с.

112 ***Махтаев М. Ш., Соловьев Л. Н.*** Применение криминалистических методик в раскрытии и расследовании преступлений в сфере компьютерной информации: Лекция. — М.: Академия ФСБ РФ, 1998. — 51 с.

113 Архив суда г. Актюбинска. Уголовное дело № 996084.

114 Архив суда г. Жезказган. Уголовное дело № 1750200.

115 Правовая информатика и кибернетика: Учебн. / Под ред. Н. С. Полевого и др. — М., 1993. — 527 с.

116 ***Федоров В.*** Компьютерные преступления: выявление, расследование // Расследование преступлений в сфере компьютерной информации: Метод. реком. — М.: НИЛ № 4 ВНИИ МВД РФ, 1998. — С. 19-22.

117 ***Григорьев М. Ю.*** «Электронная записная книжка» как новый источник получения информации при расследовании преступлений // Российский следователь. — 1999. — № 5. — С. 41-42.

118 Кодекс поведения должностных лиц по поддержанию правопорядка от 17 декабря 1979 г. (принят 34-й сессией Генеральной Ассамблеи ООН, приложен к резолюции 34/169 от 17 декабря 1979 г.) // Права человека: Сб. международ. док-тов. — М., 1998. — С. 308-309.

119 ***Силкин Л.*** Как бороться с «сетевыми» пиратами» // Российская юстиция. — 2002. — № 7. — С. 61-62.

120 Совместный Приказ председателя Комитета национальной безопасности Республики Казахстан от 20 сентября 2004 г. № 179 и и. о. председателя Агентства Республики Казахстан по информатизации и связи «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» от 20 сентября 2004 г. № 199-п.

121 ***Макоренков Д. Е., Наумов И. А.*** Получение информации из компьютерных систем в оперативно-розыскной деятельности правоохранительных органов // Информация правоохранительных систем: Тез. докл. международ. конф. (июнь, 1999 г.). — М., 1999. — С. 75.

122 ***Ищенко П. П.*** Роль специалиста-криминалиста в повышении эффективности первоначального этапа расследования // Теория и практика использования специальных знаний при расследовании преступлений. — Волгоград, 1989. — С. 15-18.

123 Устав уголовного судопроизводства 1864 г. Ст. 326 // Российское законодательство X-XX веков. Судебная реформа / Под ред. О. И. Чистякова. — М., 1991. Т. 8. — 495 с.

124 ***Ищенко П. П.*** Специалист в следственных действиях. Уголовно-процессуальные и криминалистические аспекты: Практ. пос. — М., 1990. — 158 с.

125 ***Махов В. Н.*** Участие специалиста в следственных действиях. — М., 1975. — 83 с.

126 Советский энциклопедический словарь / Под ред. А. М. Прохорова. — М., 1981. — 1600 с.

127 ***Байжанова Г. К.*** Теория и практика собирания доказательств, отображающих биологические свойства и признаки живого лица, в уголовном процессе: Дис. … канд. юрид. наук. — Караганда, 2000. — 165 с.

128 Приказ МВД СССР «О мерах по совершенствованию деятельности экспертно-криминалистических подразделений ОВД» от 5 августа 1988 г. № 170.

129 ***Казиев З. Г.*** Некоторые проблемные вопросы статуса специалиста в уголовном судопроизводстве // Законотворчество и правоприменение в Республике Казахстан. — Караганда, 1997. — С. 114-117.

130 ***Адоян Ю. А.*** О сфере деятельности специалиста в уголовном процессе // Использование специальных знаний в уголовном процессе. — Трату, 1989. — С. 82-85.

131 ***Бычкова С. Ф.*** УПК РК. Институт СЗ. НПК. — Алматы, 2000. Вып. 2. — 204 с.

132 ***Толеубекова Б. Х.*** Уголовно-процессуальное право Республики Казахстан. Часть общая: Курс лекций. — Караганда, 1994. Книга вторая. — 184 с.

133 ***Шиканов В. И.*** Проблемы использования специальных познаний и научно-технических новшеств в уголовном судопроизводстве: Автореф. дис. … канд. юрид. наук. — М., 1980. — 43 с.

134 Архив суда г. Караганда. Уголовное дело № 0503240065.

135 ***Повезнюк Г. И.*** Пределы деятельности и компетенция специалиста в следственных действиях // Бюллетень СД МВД РК. — Астана, 2000. № 5. — С. 200-217.

136 ***Арсеньев В. Д., Заблоцкий В. Г.*** Использование специальных знаний при установлении фактических обстоятельств уголовного дела. — Красноярск, 1986. — 45 с.

137 ***Орлов Ю. К.*** Заключение эксперта и его оценка по уголовным делам. — М., 1995. — 75 с.

138 ***Филимонов Б. А.*** Основы теории доказательств в германском уголовном процессе. — М., 1994. — 96 с.

139 ***Орлов Ю. К.*** Производство экспертизы в уголовном процессе: Учеб. пос. — М., 1982. — 79 с.

140 ***Селиванов Н. А.*** Привлечение специалистов к расследованию. — М., 1973. — 54 с.

141 ***Махов В. Н.*** Теория и практика использования знаний сведущих лиц при расследовании преступлений: Автореф. дис. …. д-ра юрид. наук. — М., 1993. — 54 с.

142 ***Циркаль В. В.*** Тактика производства следственных действий с участием специалистов: Автореф. дис. ... канд. юрид. наук. — Киев, 1984. — 25 с.

143 ***Аубакиров А. Ф., Гинзбург А. Я., Лившиц Ю. Д.*** Значение экспертизы в расследовании преступлений: Учеб.-метод. пос. — Караганда, 1991. — 99 с.

144 ***Мельникова Э. Б.*** Участие специалиста в следственных действиях. — М., 1964. — 215 с.

145 ***Тертышник В. М.*** Доказательства и доказывание в советском уголовном процессе: Фондовая лекция. — Харьков, 1992. — 80 с.

146 Архив суда г. Караганда. Уголовное дело № 0303200345.

147 ***Дильбарханова Ж. Р.*** Некоторые вопросы процессуального положения специалиста // Проблемы развития судебно-экспертной системы РК: Мат-лы круглого стола. — Алматы, 2004. — С. 77-79.

148 ***Ахпанов А. Н.*** Проблемы уголовно-процессуального принуждения в стадии предварительного расследования: Автореф. дис. ... д-ра юрид. наук. — М., 1997. — 50 с.

149 ***Петрухин И. Л.*** Экспертиза как средство доказывания в советском уголовном процессе. — М., 1964. — 265 с.

150 ***Кипнис Н. М.*** Допустимость доказательств в уголовном судопроизводстве. — М., 1995. — 128 с.

151 ***Грамович Г. И.*** Основы криминалистической техники. — Минск, 1981. — 158 с.

152 ***Глотов О. М.*** Формы использования специальных познаний в советском уголовном процессе должны быть расширены // Вопросы экспертизы в работе защитника. — Л.,1970. — С. 51.

153 Архив суда г. Караганда. Уголовное дело № 0603409958.

154 ***Адашкин А.*** Проведение судебно-медицинского исследования не должно служить основанием для отвода эксперта // Российская юстиция. — 2002. — № 2. — С. 54-55.

155 ***Зуев Е. И.*** Совершенствовать законодательство о специалисте и эксперте // Советская милиция. — 1975. — № 3. — С. 22-24.

156 ***Быховский И. Е.*** Совершенствование процесса доказывания на предварительном следствии // Актуальные проблемы доказывания: Сб. тезисов выступлений на теоретическом семинаре 27 марта 1981 г. — М., 1983. — С. 39.

157 Архив суда г. Караганда. Уголовные дела № 0303200064, № 0303180018, № 0503240001, № 0403240501, № 0403240469.

158 ***Вареникова С П.*** Применение специальных знаний в уголовном судопроизводстве РК: Учеб. пос. — Алматы, 2004. — 200 с.

159 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.

160 Закон Республики Казахстан «О лицензировании» от 17 апреля 1995 г. № 2200 (с изменениями от 8 мая 2003 г.) // Ведомости парламента РК. — 2003. — № 10. — С. 67-78.

161 Инструкция о порядке производства судебных экспертиз в Казахском Научно-исследовательском институте судебных экспертиз. Утверждена Министром юстиции Казахской ССР 15 мая 1981 г.

162 Постановление Правительства Республики Казахстан «Об утверждении Правил импорта, экспорта, реализации и использования специальных технических средств для проведения специальных оперативно-розыскных мероприятий, а также специальных материалов и оборудования для их производства в Республике Казахстан» № 1247 от 26 сентября 2001 г. // Официальная газета. 2001. 13 окт.

163 Проблемы развития судебно-экспертной системы РК: Мат-лы. круглого стола. — Алматы, 2004. — 110 с.

164 Информация о преступлениях в сфере высоких технологий. — М.: ГИЦ МВД РФ, 1999. — 7 с.

165 Работа судебно-экспертных учреждений в 2001 г. / Управление судебно-экспертных учреждений Министерства Юстиции России // Российская юстиция. — 2002. — № 7. — С. 80.

166 ***Гусев А.*** Высокие технологии для судебных экспертиз // Российская юстиция. — 2002. — № 7. — С. 53-55.

167 Криминалистика и компьютерная преступность // Генеральная Прокуратура РФ: Мат-лы межведомственного семинара. — М., 1993. — С. 56-68.

168 ***Селиванов Н.*** Проблемы борьбы с компьютерной преступностью // Законность. — 2002. — № 8. — С. 36-37.

169 ***Батурин Ю. М.*** Проблемы компьютерного права. — М., 1991. — 271 с.

170 Постановление Правительства Республики Казахстан «Некоторые вопросы судебной экспертизы» от 7 ноября 2001 г. № 1414 // САПП РК. — 2001. — № 39. — С. 497.

171 ***Повезнюк Г. И.*** Судебная экспертиза: Практ. пос. — Алматы, 2001. — 204 с.

172 ***Российская Е. Р.*** Судебная экспертиза в уголовном, гражданском, арбитражном процессе. — М., 1996. — 224 с.

173 Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. — М., 1999. — 254 с.

174 Пособие для следователя: Расследование преступлений повышенной опасности / Под ред. Н. А. Селиванова и А. И. Дворкина. — М., 1998. — 444 с.

175 Методическое пособие по расследованию преступлений в сфере компьютерной информации и осуществлению прокурорского надзора за исполнением законов при их расследовании. — М., 2001. — 44 с.

176 ***Бычкова С. Ф.*** Организация назначения и производства судебной экспертизы: Учеб. пос. — Алматы, 1999. — 272 с.

177 ***Крылов В. В.*** Расследование преступлений в сфере информации. — М., 1998. — 264 с.

178 Справка о результатах работы ОВД по борьбе с компьютерными преступлениями. Контрольно-методическое Управление СК МВД РФ. — М., 2001. — 16 с.

179 ***Цоколова О. И., Савкин А. В.*** Квалификация и доказывание деяний, совершаемых в сфере компьютерной информации: Метод. реком. — М., 1997. — 21 с.

ПРИЛОЖЕНИЕ А

Анкета по уголовному делу

1. Уголовное дело, следственный № _____ судебный № _____
   по обвинению Ф.И.О._____
   в совершении преступления предусмотренного ч.___ ст._____ УК

2. Наименование органа, в котором проводилось расследование _____
_____

3. Краткая фабула дела _____
_____

4. Дата поступления сообщения, заявления _____

5. Дата возбуждения уголовного дела ____ _____

6. Кем возбуждено уголовное дело.
   - следователем 001
   - органом дознания..... 002
   - прокурором 003
   - судом 004

7. Осмотр производился:
   - с участием специалиста 005
   - без участия специалиста 006

8. Участие специалиста в осмотре обусловлено:
   - специфичностью объекта исследования 007
   - решением следователя 008
   - нормой закона 009

9. Осмотр компьютерной техники производился:
   - на месте совершения преступления 010
   - в подразделении ОВД 011
   - самостоятельно специалистом 012
   - с участием понятых 013
   - без участия понятых 014

10. При внешнем осмотре компьютерной техники в протоколе:
- указываются только основные составляющие компьютера, инвентарные номера (если имеются), особенности внешнего вида 015
- указываются основные составляющие, номера, название плат, чипов, установленных в системном блоке 016

11. При осмотре программного обеспечения:
- указываются программы, запускающиеся при включении компьютера и названия просматриваемых каталогов, папок 017
- указываются все программы, установленные на винчестере, содержание всех каталогов, папок, перечень запускаемых программ за последний день (час, иной период) 018
- проверяется работа интересующих программ, особенности их запуска, связь с периферийными устройствами 019

12. При осмотре, интересующая следствие информация скопирована:
- на 1 дискету 020
- на 2 дискеты 021

13. Специалист принимал участие при расследовании преступления:
- только при производстве первоначальных следственных действий 022
- при производстве дополнительных осмотров объектов 023
- для дачи справочно-консультативной информации 024
- при производстве экспертизы 025

14. Пояснения специалиста по поводу проводимых им исследований оформлены:
- справкой 026
- протоколом допроса 027
- приложением к протоколу следственного действия 028
- иным документом (указать каким) 029

15. Прослушивание (перехват сообщений) производилось:
- исходя из тактических соображений 030
- в связи со следственно-оперативной необходимостью 031
- согласно указаниям прокурора 032
- в связи с заявлением участников процесса 033

16. Перехват сообщений, прослушивание санкционировалось:
- районным прокурором 034
- городским прокурором 035
- прокурором области 036

– генеральной прокуратурой 037

17. Прослушивание (перехват сообщений) производилось в отношении:
– подозреваемого 038
– обвиняемого 039
– потерпевшего (свидетеля) 040
– других лиц (укажите) 041

18. Результаты прослушивания, перехвата сообщений передавались следователю:
– каждые 3 дня 042
– 1 раз в неделю 043
– 1 раз в месяц 044
– после каждого перехваченного сообщения 045

19. Прослушивание, просмотр перехваченной информации проводился следователем:
– с участием специалиста 046
– с участием понятых 047
– самостоятельно 048

20. При назначении судебно-технологической (компьютерной) экспертизы исследовалось:
– конструкция компьютера, магнитных носителей, компьютерных сетей и их работа 049
– программное обеспечение, информация, хранящаяся в компьютере и на магнитных носителях 050

21. По результатам экспертного исследования получены:
– ответы на все вопросы, поставленные следователем 051
– исследование не было произведено всесторонне в связи с отсутствием специальной аппаратуры 052
– исследование не было произведено всесторонне в связи с отсутствием специалистов, могущих осветить отдельные положения 053

22. Результаты перехвата, прослушивания, судебно-технологической экспертизы:
– имели тактическое значение 054
– позволили установить лиц, интересующих следствие 055
– позволили обнаружить новые источники информации 056
– не использованы при расследовании преступления 057
– использованы в качестве обвинительных доказательств 058

23. При приостановлении производства по уголовному делу перехват сообщений, прослушивание:
- приостанавливалось 059
- не приостанавливалось 060
- не указано 061

24. Результаты расследования:
- прекращено (основания п. ___ ст. ___УПК) 062
- приостановлено (основание п. ___ ст. ___УПК) 063
- вынесен обвинительный приговор 064
- вынесен оправдательный приговор 065
- к лицу применены принудительные меры медицинского характера 066

25. Возраст обвиняемого:
- от 14 до 16 лет 067
- от 16 до 18 лет 068
- от 18 до 25 лет 069
- от 25 до 35 лет 070
- от 35 до 55 лет 071
- свыше 55 лет 072

26. Пол и семейное положение:
- мужской 073
- женский 074
- холост (незамужем) 075
- женат (замужем)..... 076
- одинокий 077

27. Образование:
- высшее 078
- неоконченное высшее 079
- среднее 080
- среднее специальное 081
- неоконченное среднее 082
- начальное 083
- не имеет образования 084

28. Род занятий:
- рабочий 085
- служащий 086
- студент 087

– учащийся 088
– коммерсант 089
– безработный 090
– лицо без определенного рода занятий 091

29. Место жительства, гражданство:
– местный житель 092
– приезжий 093
– лицо, без определенного места жительства 094
– гражданин Республики Казахстан 095
– гражданин другого государства (укажите какого) 096
– лицо, без гражданства 097

30. Преступление совершено:
– трезвым 098
– в состоянии алкогольного опьянения 099
– в состоянии наркотического опьянения 100
– в одиночку 101
– в группе лиц 102

31. Наличие судимости:
– не судим 103
– судим за тяжкое преступление 104
– судим более 3-х раз 105
– признан ООР 106

32. Предъявлена характеристика:
– по месту жительства 107
– по месту работы 108
– положительная 109
– отрицательная 110
– отсутствует 111

ПРИЛОЖЕНИЕ Б

Опросный лист

Уважаемый коллега!

Ваши ответы на поставленные вопросы способствуют изучению проблемы реализации перехвата сообщений с компьютерных систем и технических каналов связи, введенного в действие в 1998 г. в сферу уголовного судопроизводства Республики Казахстан.

Это исследование проводится исключительно в научных целях, и собранные данные будут использованы только в обобщенном виде.

Просим Вас выделить (подчеркнуть, округлить) те ответы, с которыми согласны. Правильных ответов может быть несколько, если ни один из ответов вас не устраивает, напишите свое мнение.

Заранее благодарим Вас за сотрудничество!

1. Под перехватом сообщений Вы понимаете:
   - копирование передаваемой информации 001
   - изъятие информации 002
   - блокирование информации 003
   - все вышеперечисленные положения 004
   - иное (укажите)_____ 005

2. Как Вы считаете, с какой целью производится перехват сообщений:
   - получения интересующей информации 006
   - выяснения возможности лица, использовать компьютерную сеть, в качестве средства связи 007
   - обнаружения новых источников информации 008
   - иное (укажите)_____ ... 009

3. Сталкивались ли Вы с необходимостью производства перехвата сообщений в своей деятельности?
   - да 010
   - нет 011

4. Как Вы считаете, необходимо ли дополнить юридическое основание производства перехвата сообщений (указанного в УПК — постановления, санкционированного прокурором), фактическими основаниями?
   – да 012
   – нет 013
   – иное (укажите) _____ ... 014

5. Осуществление перехвата сообщений может быть поручено:
   – спецподразделениям МВД 015
   – спецподразделениям КНБ 016
   – провайдерам, осуществляющим реализацию услуг в сфере компьютерных технологий 017
   – иное (укажите) _____ ... 018

6. Как Вы считаете, необходима ли норма, определяющая сроки хранения информации у провайдеров, о пользователях их адресах, отправляемых и получаемых ими сообщений:
   – да 019
   – нет 020
   – иное (укажите) _____ 021

7. Как Вы считаете, какова должна быть продолжительность срока производства перехвата сообщений:
   – 1 месяц 022
   – менее 1 месяца 023
   – аналогично сроку расследования 024
   – может носить разовый характер 025
   – иное (укажите) _____ ... 026

8. Если при реализации перехвата сообщений к органу уголовного преследования попала информация о частной жизни лица, то он должен:
   – вернуть информацию владельцу 027
   – скопировать информацию и хранить ее в деле 028
   – если она имеет значение для дела, принять меры к недопустимости ее разглашения и, скопировав, хранить в установленном законом порядке 029

9. Как Вы считаете, к кому может применяться перехват сообщений?
   – обвиняемому 030
   – подозреваемому 031
   – свидетелю (потерпевшему) 032
   – иным лицам (укажите) 033

10. Считаете ли Вы, что компьютерная информация и электронный документ — тождественные понятия?
    - да 034
    - нет 035
    - иное (укажите) _____ 036

11. Как Вы считаете, необходимо ли единое трактование терминов, «компьютерная сеть», «каналы связи», «линия связи», «компьютерная информация», «машинограмма» в сфере уголовного судопроизводства:
    - да 037
    - нет (не имеет значения при составлении процессуальных документов) 038
    - иное (укажите) _____ 039

12. Как Вы считаете, имеет ли компьютерная информация, полученная при перехвате сообщений в ходе производства ОРД, доказательственное значение?
    - да 040
    - нет (только ориентирующее) 041
    - иное (укажите) _____ 042

13. При осмотре полученной информации, необходимо ли указывать материальный носитель, ее реквизиты, перечень имеющихся файлов, содержание информации, используемое программное обеспечение:
    - да 043
    - нет (достаточно указать содержание перехваченной информации) 044
    - иное (укажите) _____ 045

14. Представляет ли для Вас сложность осмотр компьютера, с целью обнаружения интересующей информации.
    - да (укажите, в чем она выражается) _____ 046
    - нет 047

15. Как часто Вы обращаетесь к специалистам для получения справочно-консультативной помощи?
    - по каждому расследуемому делу 048
    - очень редко 049
    - не обращаюсь 050
    - иное (укажите) _____ 051

16. Чем, по Вашему мнению, обусловлено участие специалиста в осмотре и работе с компьютерной техникой и информацией?
   – обязательным его участием в соответствии с законом 052
   – отсутствием у Вас навыков работы с компьютерной техникой .. 053
   – с целью более качественного исследования информации 054
   – тактическими особенностями производства следственного действия 055
   – иными обстоятельствами (укажите) _____ 056

17. Сталкивались ли Вы с той ситуацией, когда первоначальное участие специалиста не дало Вам возможности использовать его знания и навыки при дальнейшем расследовании дела?
   – да 057
   – нет 058

18. Необходимо ли разрешить привлечение специалистов редких профессий и узкой специализации не только к участию в следственных действиях, но и к производству экспертиз, несмотря на их предыдущее участие в деле?
   – да 059
   – нет 060

19. Проводимое исследование специалиста оформляется:
   – протоколом проводимого следственного действия 061
   – протоколом исследования специалиста 062
   – иным документом (укажите) _____ 063

20. Приходилось ли Вам назначать судебно-технологическую (компьютерную) экспертизу?
   – да 064
   – нет 065

21. Возникали ли у Вас трудности при назначении судебно-компьютерной экспертизы с определением границ исследования, формулировкой вопросов?
   – если да, то, что вызывало сложность при формулировании вопросов (укажите) _____ 066
   – нет 067

22. Кому поручалось производство судебно-технологической (компьютерной) экспертизы?
   – экспертам Вашего региона 068
   – экспертам других регионов 069

– специалистам 070

23. Как Вы полагаете, какие факторы препятствуют эффективному осуществлению перехвата сообщений и использованию его результатов при расследовании преступлений:
– недостаточные специальные знания сотрудников 071
– недостаточное техническое оснащение 072
– несовершенная регламентация правовой нормы 073
– иное (укажите) _____ 074

24 Ваша должность.
– следователь (ст. следователь) 075
– дознаватель (ст. дознаватель) 076
– начальник следственного отдела 077
– прокурор 078
– специалист 079
– эксперт 080
– иная (укажите) _____ 081

25. Ваше образование.
– высшее юридическое 082
– иное высшее 083
– неоконченное высшее 084
– средне специальное 085
– иное (укажите какое) _____ 086

26. Стаж работы в правоохранительных органах
– до 3 лет 087
– от 3 до 5 лет 088
– от 5 до 10 лет 089
– свыше 10 лет 090

27. Стаж следственной работы.
– до 1 года 091
– от 1 до 3 лет 092
– от 3 до 5 лет 093
– от 5 до 10 лет 094
– свыше 10 лет 095

ПРИЛОЖЕНИЕ В

ПРИЛОЖЕНИЕ Г

ПРИЛОЖЕНИЕ Д

ПРИЛОЖЕНИЕ Е

ПРИЛОЖЕНИЕ Ж

ПРИЛОЖЕНИЕ И

ПРИЛОЖЕНИЕ К

ПРИЛОЖЕНИЕ Л

ПРИЛОЖЕНИЕ М