МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

КАРАГАНДИНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
ИМЕНИ БАРИМБЕКА БЕЙСЕНОВА

А. В. Сырбу

ПЕРЕХВАТ СООБЩЕНИЙ В СИСТЕМЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Учебное пособие

«Рекомендовано» Учебно-методической секцией по специальности
«Правоохранительная деятельность»

КАРАГАНДА 2007

ББК 67.73я7
С 95

Печатается по решению ученого совета Карагандинского юридического института МВД РК им. Б. Бейсенова.

Рецензенты: начальник следственного управления ДВД Карагандинской области, подполковник полиции ***Р. Ф. Ефизов***; доцент кафедры уголовного процесса Карагандинского юридического института МВД РК им. Б. Бейсенова, кандидат юридических наук ***Н. В. Мазур***.

Сырбу А. В.

С 95 Перехват сообщений в системе следственных действий: Учебное пособие. — Караганда: Карагандинский юридический институт МВД РК им. Б. Бейсенова, 2007. — 106 с.

ISBN 9965-836-22-1

В настоящем учебном пособии рассматриваются процессуальные способы получения информации с технических каналов связи. 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.

Пособие предназначено для научных сотрудников, адъюнктов, соискателей, студентов юридических вузов, а также практических работников правоохранительных органов.

ББК 67.73я7

ISBN 9965-836-22-1

ВВЕДЕНИЕ

В настоящее время человечество находится лишь на пороге всепланетной коммуникации с использованием компьютерных технологий. Научные прогнозы предвещают невероятный рост всех видов сетей связи — спутниковых, межконтинентальных световолоконных сетей, локальных компьютерных сетей. Сотни тысяч ЭВМ, связанных между собой, будут подключены к национальным и международным сетям. Стремительное развитие информационных технологий приводит к тому, что многие явления социальной жизни все в большей мере находят отражение в так называемых «виртуальных мирах», т. е. 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 сферу применения компьютерных технологий. Развитие компьютерных технологий и международных сетей как неотъемлемой части современной международной финансовой и банковской деятельности, а также таких сфер как производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации, создало предпосылки, в немалой степени облегчающие совершение преступных деяний как внутри страны, так и на международном уровне.

В современном компьютеризованном обществе почти все преступления могут совершаться с помощью имеющейся компьютерной технологии и все расширяющейся сферы ее применения. Например, в 1999 г. в США, впервые в истории криминалистики, раскрыто убийство, при совершении которого Интернет использовался в качестве непосредственного орудия. Для физического уничтожения важного свидетеля, находившегося в госпитале после ранения, преступники через сеть Интернет проникли в локальную информационную структуру и изменили режим работы кардиостимулятора и аппарата искусственной вентиляции легких, в результате чего пациент скончался[1]. Связанные с использованием компьютеров преступления, как правило, выходят за рамки обычных и нередко представляют собой нераз-

---

[1] Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю. В. Гаврилина. — М., 2003.

решимые для действующего законодательства задачи.

Исследуя разнообразие совершаемых компьютерных преступлений, следует отметить, что большинство таких деяний носит корыстную направленность и поэтому представляет наибольшую опасность для финансовой и производственной сферы. Анализ статистики о зарегистрированных преступлениях и результатах деятельности органов уголовного преследования МВД РК, дает представление о росте выявленных преступлений с использованием компьютерной техники: так в 2004 г. совершено 3646 преступлений, в 2005 г. — 3978, за 8 месяцев 2006 г. — 2658 преступлений. Из изложенного видно, что число преступлений в сфере высоких технологий ежегодно возрастает, что связано с распространением новых информационных и телекоммуникационных технологий, а также связано с ростом числа пользователей компьютеров и средств связи. При этом следует учитывать, что 90 % преступлений в сфере высоких технологий являются латентными. Ввиду стремления преступности (прежде всего организованной) укрепить свои позиции в информационной сфере, возникает объективная необходимость в совершенствовании форм, средств и методов деятельности полиции. Назрел вопрос и о коррективах в кадровой работе, подготовке сотрудников, способных противостоять противоправным проявлениям в сфере высоких технологий.

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

В настоящем пособии сформулированы новые теоретические положения, направленные на раскрытие процессуального значения, сущности и содержания информации, передаваемой по техническим, в том числе компьютерным каналам связи, порядка ее использования; определения роли перехвата сообщений как самостоятельного следственного действия в системе следственных действий уголовно-процессуального права Республики Казахстан; а также разработка на данной основе практических рекомендаций, направленных на совершенствование законодательного регламентирования перехвата сообщений, а также практики его применения в стадиях досудебного производства, оптимизацию расследования уголовных дел.

Глава 1

ПЕРЕХВАТ СООБЩЕНИЙ КАК САМОСТОЯТЕЛЬНОЕ СЛЕДСТВЕННОЕ ДЕЙСТВИЕ

В своем Послании к народу Республики Казахстан Президент РК Н. А. Назарбаев указал, что одной из первоочередных задач, стоящих перед нашим государством, является «...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 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, находящихся на вооружении органов дознания и предварительного следствия, в целях быстрого и полного раскрытия преступлений, доказывания причастности к ним всех членов преступных групп: организаторов, исполнителей, подстрекателей и пособников.

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

---

[1] *Назарбаев Н. А.* К свободному, эффективному и безопасному обществу: Послание Президента страны народу Казахстана // Юридическая газета. 2000. 25окт.

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»[1].

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»[2].

В новом Уголовно-процессуальном кодексе Республики Казахстан предусмотрено процессуальное право органов следствия и дознания на проведение мероприятий по осуществлению контроля за передаваемыми сообщениями по техническим каналам связи.

Деятельность по получению и использованию информации с технических каналов связи, в том числе компьютерных систем, в процессе расследования преступлений должна базироваться на разработанных теоретических и правовых основах.

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 необходимостью разработки новых правовых институтов, позволяющих расширить доказательственную базу путем использования в доказывании информации, полученной с технических каналов связи, в том числе с компьютерных систем.

В уголовно-процессуальном праве предусмотрена возможность проведения нового следственного действия — «перехват сообщений», закрепленного в ст. 236 УПК РК.

---

1 Казахстан 2030: Послание Президента страны народу Казахстана. — Астана, 2000. — С. 70-97.

2 Программа действий правительства, утвержденная Указом Президента РК от 28 января 1998 г. № 3834 «О мерах по реализации Стратегии развития Казахстана до 2030 года». Казахстан 2030. — Астана 2000. — С. 32.

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.

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

Во-вторых: 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 др. 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 перед правоприменителем 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 частности, 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.

В-третьих: в уголовно-процессуальных нормах, регулирующих получение и использование информации с технических каналов связи, 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 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 по данному вопросу свидетельствует о том, что о сущности и механизме перехвата сообщений, передаваемых по техническим, в том числе компьютерным каналам связи, и снятии информации с компьютерных систем имеют представление 28 % опрошенных. При этом следует учесть, что опрос проводился среди всех категорий участников, имеющих отношение к данному действию (120 следователей, 80 дознавателей, 50 прокурорских работников, 57 специалистов, 23 экспертов и др.).

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.

В-четвертых: 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. Думается, 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 совершенствование 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.

1.1. 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 с Конституцией допустимо только в случаях и в порядке, прямо установленных законом. Такими Законами являются: Закон РК «Об Оперативно-розыскной деятельности» и Уголовно-

процессуальный кодекс. Несмотря на то, что данные Законы допускают проведение мероприятий по прослушиванию телефонных переговоров и сообщений правовой механизм использования результатов был недостаточно отрегулирован. Среди профессионалов долгое время не прекращаются споры о возможности использования в качестве доказательств в уголовном процессе результатов прослушивания переговоров и 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 1998 г., содержащего ст. 236 «Перехват сообщений». Однако отметим, что законодатель не раскрыл содержания понятия «перехват сообщений» и 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[1]».

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 ред. С. И. Ожегова мы найдем следующее толкование:

Перехват: 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, обратившись к сходным по смыслу терминам — «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[2].

---

[1] *Нургалиев Б. М., Арыстанбеков М. А.* Наложение ареста на почтово-телеграфную корреспонденцию. Перехват сообщений. Прослушивание и запись переговоров. — Караганда, 1999. — С. 174.

[2] *Ожегов С. И.* Словарь русского языка. — М., 1972. — С. 650.

Изъятие — в уголовном процессе — отчуждение (или получение) предметов или документов происходящее при производстве следственных действий[1].

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.

Вместе с тем, данная формулировка не раскрывает в полной мере процессуальное содержание перехвата сообщений, а также порядок и особенности производства операций над передаваемыми сообщениями, компьютерной информацией. Полагаем необходимым обратиться к научным исследованиям и специальной литературе в области уголовного-процессуального права, информатики и информации, определяющими порядок работы с компьютерной информацией в целях всестороннего исследования настоящего вопроса.

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»[2].

---

[1] Словарь основных уголовно-процессуальных понятий терминов / Сост. А. М. Баранов, П. Г. Марцифин. — Омск, 1997. — С. 12.

[2] Расследование преступлений повышенной общественной опасности: Пособие для следователя / Под ред. д. ю. н., проф. Н. А. Селиванова. — М., 1999.

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[1].

Говоря о блокировании информации, следует отметить, что в Законе РК «О связи» в ч. 2 ст. 9 определено: «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»[2].

Ю. Гульбин исследуя вопросы терминологии операций над информацией, под уничтожением информации понимает лишение сведений, данных и пр. соответствующей материальной формы; под блокированием — лишение возможности правомерного пользователя реализовывать информацию ЭВМ по назначению[3]».

Проанализировав различные мнения и понятия терминов, связанные с обработкой информации, предлагается универсальная, но не претендующая на роль исключительной трактовка 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

---

1 ***Крылов В. Б.*** Информационные компьютерные преступления. — М., 1997. — С. 76.

2 Закон Республики Казахстан «О связи» от 13 мая 1999 г. // Казахстанская правда. 1999. 21 мая.

3 ***Гульбин Ю.*** Преступления в сфере компьютерной информации // Российская юстиция. — 1997. — № 10. — С. 32.

скопирована на магнитный носитель. При этом в протоколе осмотра была сделана следующая запись: «...при исследовании информации, содержащейся в компьютере в папке "7567564", имеющей путь — C \ 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[1]». 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 (A)[2]».

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 хранится 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 вос-

---

1 Уголовное дело № 960710, возбужденное СС УВД г. Петропавловска по факту фальшивомонетничества с использованием персонального компьютера.

2 Уголовное дело № 1252251203 , возбужденное СС УВД по факту мошенничества.

становлена 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 др.). Файл — именованная область носителя компьютерной информации — Примеч. автора.

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 № 960710 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»[1].

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

[1] Уголовное дело № 960710, возбужденное СС УВД г. Петропавловска по факту фальшивомонетничества с использованием персонального компьютера

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.

Проведенный анализ исследуемых вопросов позволяет прийти к выводу, что, 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.

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».

1.2. Сущность и содержание перехвата сообщений

Вступление человечества в новую эру развития – век высоких технологий и электронных коммуникаций, закономерно повлекло широкое использование компьютерных технологий в различных сферах его деятельности. Развивающийся Казахстан, в соответствии с приоритетами, определенными программой «Стратегия развития Казахстана 2030 года», активно вступил на путь применения высокотехнологических наукоемких производств. Нововведения затронули и сферу уголовного судопроизводства. Принятие Уголовно-процессуального кодекса Республики Казахстан заставило поновому 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 техниче-

ских каналов связи, компьютерных систем, в том числе и при производстве оперативно-розыскных мероприятий.

Рассматривая сущность перехвата сообщений, введенного Уголовно-процессуальным кодексом Республики Казахстан 1998 года, невольно возникает вопрос: с чем связано появление нового следственного действия и чем оно отличается от уже действующих? Проводя анализ, можно прийти 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 в форме таблицы.

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

Обыск (ст. ст. 230, 232, 233 УПК)	**Перехват сообщений (ст. 236 УПК)**	**Прослушивание телефонных переговоров (ст. 237 УПК)**
Цель — обнаружение и изъятие предметов или документов, имеющих значение для дела. **Объект исследования** — помещения, земельные участки, вещи, предметы, и др. **Метод** — допустимо принудительное проникновение, использование взлома преград. **Предмет исследования** — любые объекты, имеющие значение для дела. **Срок действия** — разовый **Санкция прокурора** — обязательна, но есть исключительные случаи. **Участие специалиста** — необходимость определяется следователем	**Цель** — обнаружение информации, передаваемой по техническим, компью- **Объект исследования** — компьютерная система, компьютерная сеть, технические каналы связи. **Метод** — использование спец.средств, взлом не предусмотрен, но может быть допустим, при наличии пароля на сообщение. **Предмет исследования** — информация, относящаяся к расследуемому делу. **Срок действия** — не определен, но может быть разовым или продолжительным **Санкция прокурора** — обязательна **Участие специалиста** — необходимо	**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. **Срок действия** — продолжительный (до 6 месяцев) **Санкция прокурора** — обязательна, но есть исключительные случаи. **Участие специалиста** — необходимо

Из приведенной таблицы 1 видно, что перехват сообщений включает в себя как положения обыска, так и прослушивания 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, машина, контора, личные вещи и бумаги). Нарушение этого запрета приводило к исключению из рассмотрения судом незаконно изъятых вещественных доказательств, т. е. суды отождествляли право собственности индивида и сферу его частной жизни.

Появление электронных подслушивающих и звукозаписывающих устройств предоставило возможность правоохранительным органам «изымать» мысли, желания, надежды, намерения граждан, воплощенные в слова, т. е. 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-технической революции является выработка стандартов и создание процедур, гарантирующих право на частную жизнь.

Идея «общего обыска» наиболее ощутимо проявляется в практике прослушивания и электронного наблюдения с целью перехвата и фиксации разговоров граждан на основе предписаний статутов и повседневной практике полицейских органов.

Юристы утверждали, что подслушивание должно быть приравнено к проведению обыска изъятия, так как по своей сути оно мало чем отличается от обыска с целью изъятия доказательств преступления. 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

ских каналов связи, компьютерных систем, в том числе и при производстве оперативно-розыскных мероприятий.

Рассматривая сущность перехвата сообщений, введенного Уголовно-процессуальным кодексом Республики Казахстан 1998 года, невольно возникает вопрос: с чем связано появление нового следственного действия и чем оно отличается от уже действующих? Проводя анализ, можно прийти 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 в форме таблицы.

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

Обыск (ст. ст. 230, 232, 233 УПК)	**Перехват сообщений (ст. 236 УПК)**	**Прослушивание телефонных переговоров (ст. 237 УПК)**
Цель — обнаружение и изъятие предметов или документов, имеющих значение для дела.	**Цель** — обнаружение информации, передаваемой по техническим, компью-	**Цель** — обнаружение сведений, имеющих значение для дела.
Объект исследования — помещения, земельные участки, вещи, предметы, и др.	**Объект исследования** — компьютерная система, компьютерная сеть, технические каналы связи.	**Объект исследования** — телефонные лини связи, переговорные устройства.
Метод — допустимо принудительное проникновение, использование взлома преград.	**Метод** — использование спец.средств, взлом не предусмотрен, но может быть допустим, при наличии пароля на сообщение.	**Метод** — использование прослушивающих и записывающих устройств.
Предмет исследования — любые объекты, имеющие значение для дела.	**Предмет исследования** — информация, относящаяся к расследуемому делу.	**Предмет исследования** — информация, представляющая интерес для расследования.
Срок действия — разовый	**Срок действия** — не определен, но может быть разовым или продолжительным	**Срок действия** — продолжительный (до 6 месяцев)
Санкция прокурора — обязательна, но есть исключительные случаи.	**Санкция прокурора** — обязательна	**Санкция прокурора** — обязательна, но есть исключительные случаи.
Участие специалиста — необходимость определяется следователем	**Участие специалиста** — необходимо	**Участие специалиста** — необходимо

Из приведенной таблицы 1 видно, что перехват сообщений включает в себя как положения обыска, так и прослушивания 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, машина, контора, личные вещи и бумаги). Нарушение этого запрета приводило к исключению из рассмотрения судом незаконно изъятых вещественных доказательств, т. е. суды отождествляли право собственности индивида и сферу его частной жизни.

Появление электронных подслушивающих и звукозаписывающих устройств предоставило возможность правоохранительным органам «изымать» мысли, желания, надежды, намерения граждан, воплощенные в слова, т. е. 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-технической революции является выработка стандартов и создание процедур, гарантирующих право на частную жизнь.

Идея «общего обыска» наиболее ощутимо проявляется в практике прослушивания и электронного наблюдения с целью перехвата и фиксации разговоров граждан на основе предписаний статутов и повседневной практике полицейских органов.

Юристы утверждали, что подслушивание должно быть приравнено к проведению обыска изъятия, так как по своей сути оно мало чем отличается от обыска с целью изъятия доказательств преступления. 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

ордер 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 века 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[1].

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

[1] Полномочия прокурора при досудебном производстве и рассмотрении дела судом определяются соответственно статьями 190, 192 (частями шестой и седьмой), 197, 289, 317, 396 (частью третьей), 458, 460 УПК РК.

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.

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 сделано в деле Олмстеда (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 право-

применительных 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 Федерального 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 показания 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, Федеральный 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, присоединившись к мнению большинства в деле Сильвермана, тем не менее 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.

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 содер-

жимое его разговора останется в тайне»[1]. 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 решения по делу Каца, на основании 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 предпринята 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 т. д.). Для подслушивания в иных мес-

[1] Трактовка поправки IV к Конституции США, разрабатываемая Верховным судом США в 1964-65 гг.

тах, например, в тюрьме, ордер не требовался (§ 2510 /2/). Во втором случае прослушивание без ордера вообще запрещалось (§ 2510 /11/).

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.

Думается, 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 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 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, необходимо определить процессуальный порядок производства перехвата сообщений и более детально остановиться на каждом из аспектов его реализации.

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.

1.3. Цели, основания и условия реализации 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[1].

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»[2].

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.

Так, 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».

---

1 ***Овчинский С. С.*** Оперативно-розыскная информация. Теоретические основы информационно-прогностического обеспечения оперативно-розыскной и профилактической деятельности ОВД по борьбе с организованной преступностью. — М., 2000. — С. 311.

2 ***Акчурин А. Г., Акчурин А. А.*** Многофакторный анализ компьютерных преступлений // Казахстан-2030. Проблемы совершенствования деятельности правоохранительных органов. — Алматы, 1999. — С. 386.

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. Принятый в 1968 г. Федеральный Закон «О контроле над преступностью и обеспечения безопасности на улицах», окончательно легализовал электронное подслушивание с разрешения и под контролем судебных органов для расследования многих тяжких преступлений — взяточничества, похищения людей, незаконной торговли наркотиками, убийств, грабежей, игорного бизнеса. В законе также была 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 компьютерной криминальной информации представляется чрезвычайно актуальной. Широкое использование для обработки информации локальных и глобальных вычислительных сетей делает чрезвычайно перспективным разработку соответствующих методов получения информации. Актуальность данного исследования подтверждается введением Уголовно-процессуальным кодексом Республики Казахстан 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.

Необходимость исследования и разработки правил производства перехвата сообщений 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 по-

лученной таким образом информации. Данный критерий и процессуальный кодекс, о котором говорилось выше, должны быть преданы гласности»[1].

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»[2]. 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, 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 т. д.

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 УПК РК (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, т. к. 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» очевидно 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

---

1 ***Аксель Хорн и Ульф Мюллер.*** Выдержки из полного отчета отдела Европейского парламента по оценке научно-технологических разработок «Оценка технологий политического контроля». 4 февраля 1998 г. ohttp://jva.com/stoa-atcp.htm (505 k 26 января 1998 г.

2 Теория доказательств в советском уголовном процессе. — М., 1973. — С. 383.

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 «Прослушивание и запись переговоров» УПК РК 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. Думается, 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»[1].

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

---

[1] ***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.

Следует полагать, 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 будет 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). Следует 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[1].

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

По мнению К. Ж. Капсалямова[2], фактическим основанием для перехвата сообщений являются достаточные данные полагать, 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,

---

[1] Уголовное дело № 216001 по факту неправомерного доступа в локальную сеть Актюбинского РИВЦ, возбужденное вторым отделом 4-го Управления ДКНБ РК по Актюбинской области.

[2] ***Капсалямов К. Ж.*** Уголовное преследование и способы собирания доказательств. — Астана, 2001. — С. 64-66.

полученные в ходе оперативно-розыскных мероприятий, регламентированных ст. 11 Закона РК «Об оперативно-розыскной деятельности». 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[1]. 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[2]. В пункте 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.

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

---

1 *Чувилев А. Н.* Процессуальные основания и порядок прослушивания и звукозаписи телефонных и иных переговоров в уголовном судопроизводстве. — М., 1999. — С. 107.

2 Рекомендации по применению средств видео-, звукозаписи, кинофотоаппаратуры, телефонной связи и использовании полученных результатов при предотвращении, раскрытии и расследовании преступлений. — М., 1990. Прокуратура СССР (№1/2948 от 23 июня 1990 г.).

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 в тайне 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 преступность...»[1], что «допускается прослушивание без ордера, если хотя бы один из участников разговора добровольно разрешает сделать это».

Хотелось бы обратить внимание на то, что в УПК ФРГ[2] закреплена статья — «Основания для контроля телефонных переговоров», в которой законодатель устанавливает следующие основания 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, поддел-

---

1 Закон «О контроле над преступностью и обеспечением безопасности на улицах» 19 июня 1968 г. Третий раздел закона «Подслушивание телефонных переговоров и электронное прослушивание». Глава 1 119 // Законодательство зарубежных стран. Обзорная информация. — М., 1982.

2 УПК Федеративной Республики Германия &98.

ка денег или ценных бумаг, похищение людей, убийство, разбой, преступление предусмотренное законом о наркотиках.

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»[1] 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. Соотношение возможности осуществления указанных оперативно-розыскных мероприятий со степенью тяжести противоправного деяния указывает на вынужденных характер их проведения, а также позволяет правоприменителю использовать Особенную часть УК РФ для ограничения конституционных прав граждан»[2].

Учитывая больший опыт зарубежных стран, в целях недопущения и устранения пробелов, могущих возникнуть в 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

---

1 Федеральный Закон Российской Федерации «Об оперативно-розыскной деятельности в РФ».

2 О последних изменениях оперативно-розыскного и уголовно-процессуального законодательства, касающихся контроля и записи телефонных и иных переговоров // Российский следователь. — 2002. — № 5. — С. 21.

«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:

«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 де-

ла, 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».

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»[1].

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;

[1] *Батурин Ю. М., Жодзишский А. М.* Компьютерная преступность и компьютерная безопасность. — М., 1991. — С. 124.

– 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,[1] 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[2]. Следовательно, решение прокурора о назначении перехвата сообщений является обязательным для исполнения и входит 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

[1] 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 статьями 190, 192 (частями шестой и седьмой), 197, 289, 317, 396 (частью третьей), 458, 460 УПК РК.

[2] «Указания прокурора следователю… дознавателю, данные в порядке предусмотренном УПК, являются обязательными, но могут быть обжалованы вышестоящему прокурору, обжалование полученных указаний вышестоящему прокурору не приостанавливает их исполнение». Часть 2 ст. 197 УПК РК в редакции Закона РК № 163-11 от 16.03.01.

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,[1] 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

---

[1] 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 т. д.

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 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.

В качестве примера предлагается разработанный автором образец постановления о перехвате сообщений, опубликованный в «Примерных образцах уголовно-процессуальных актов досудебного производства»[1].

«Перехват сообщений по компьютерным
каналам связи с 20 марта 200_ года по
20 мая 200_ года, сроком на 2 месяца
«САНКЦИОНИРУЮ»
Прокурор г. Энска советник юстиции 1 класса
И. З. Гуслав
20 марта 200_ года

ПОСТАНОВЛЕНИЕ
о перехвате сообщений по компьютерным каналам связи

20 марта 200__ года г. Энск

Следователь Со г.Энска лейтенант полиции Фролов Н. Н., рассмотрев материалы уголовного дела № 99776000

---

[1] Примерные образцы уголовно-процессуальных актов досудебного производства / Под общ. ред. А. Н. Ахпанова, Т. Е. Сарсенбаева. — Астана, 2000. — С. 206.

УСТАНОВИЛ:

В период с 10.12.200_ года по 20.04.2000_ года гражданин Рерих Р. Р. организовал преступную группу, совершившую 5 убийств, 10 разбойных нападений и 15 краж.

При подготовке к совершению преступлений, а также при реализации вещей и предметов, добытых преступным путем, Рерих Р. Р. связывался с сообщниками посредством компьютерного канала связи, по адресу электронной почты «rotary@rrr.kaz», подключенного к компьютеру «Pentium-III», находящегося у его сестры Рерих И.Р., проживающей по адресу: г. Энск, ул. Гоголя, д. 45, кв. 44, через сервер провайдера ОАО «Казахтелеком».

На основании изложенного и учитывая, что в результате перехвата сообщений, получаемых по компьютерному каналу связи, может быть получена информация, имеющая значение для дела, в том числе для установления и изобличения виновных лиц, руководствуясь ч. 5 ст. ст. 236, 202 УПК РК,

ПОСТАНОВИЛ:

1. Произвести перехват сообщений, получаемых по компьютерному каналу связи, адрес электронной почты «rotary@rrr.kaz», подключенного к компьютеру находящемуся по адресу: г. Энск, ул. Гоголя 45-44, сроком на 2 месяца, т. е. до 20 мая 200__ года.
2. Производство перехвата сообщений по компьютерному каналу связи и их запись поручить специалистам ОАО «Казахтелеком» по Энской области.
3. В соответствии с требованиями ст. ст. 53 и 205 УПК РК разъяснить руководителю и специалистам ОАО «Казахтелеком», осуществляющим перехват сообщений, о сохранении конфиденциальности и об уголовной ответственности по ст. 355 УК РК за разглашение данных предварительного расследования.
4. Копию настоящего постановления вручить руководителю ОАО «Казахтелеком» для исполнения.
5. Копию настоящего постановления направить прокурору г. Энска.

Следователь СО ОВД
г. Энска
лейтенант полиции Фролов Н. Н.

Копию постановления вручена руководителю ОАО «Казахтелеком» по Энской области 20.03.200__ г.

Копию постановления направлена прокурору г. Энска, исх. № 845 от 20.03.200__ г.

Об уголовной ответственности по ст. 355 УК РК за разглашение данных предварительного расследования предупреждены.

Руководитель ОАО «Казахтелеком» _____

Специалисты _____

_____

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, предлагается:

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 использование ее при расследовании преступлений.

Объектом перехвата сообщений являются - компьютерная система, компьютерная сеть, технические каналы связи, исследование которых позволит органу уголовного преследования получить относимую 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. 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 по юридическим (постановления) и фактическим (оперативно-розыскная информация, заявления участников уголовного процесса и другие доказательства, полученные по уголовному делу) основаниям.

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

Дополнить ст. 236 УПК РК частями следующего содержания:

«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.

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.

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».

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».

1.4. 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 течении 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 юридического факта либо элемента сложного юридического состава, иначе говоря, 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 дисциплинарного 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.

До периода бурного развития технических средств электронного наблюдения и подслушивания, запрет необоснованных обысков, как гарантия соблюдения прав граждан на частную жизнь, распространялся только на материальные объекты (дом, машина, контора, личные вещи и бумаги). Нарушение этого запрета приводило к исключению из рассмотрения судом незаконно изъятых вещественных доказательств, т. е. суды отождествляли право собственности индивида и сферу его частной жизни. Появление электронных подслушивающих и звукозаписывающих устройств предоставило возможность правоприменительным органам «изымать» желания, намерения граждан, воплощенные в слова, т.е. все то, что формирует частную жизнь гражданина. 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».

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[1] 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». В статье 99 УПК ФРГ «компетентный орган контроля за телефонными переговорами», в ч. 2 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». 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»[2]. 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

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г.

[2] Закон «О контроле над преступностью и обеспечением безопасности на улицах». Принят Конгрессом США 19 июня 1968 г.

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 получения информации с технических каналов связи 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»[1].

Дальнейшее продление первоначального срока производства перехвата сообщений, 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 чч. 4, 5 ст. 196 УПК РК.

Кроме изложенного выше «продолжительного» срока, полагаем, что перехват сообщений может носить «разовый» характер.

В качестве примера можно указать, что при изучении уголовных дел, связанных с назначением перехвата сообщений, практически по всем из них следователи не указывали в резолютивной части постановления конкретные сроки перехвата сообщений, ограничиваясь формулировкой: «1. Произвести перехват сообщений, получаемых по компьютерному каналу связи, адрес электронной почты «XXX.kaz», подключенного к компью-

[1] Комментарий к Уголовно-процессуальному кодексу Казахской ССР по состоянию на 15 мая 1995 г. — Алматы, 1995. — С. 257.

теру находящемуся по адресу «Р». 2. Производство перехвата сообщений по компьютерному каналу связи и их запись поручить сотрудникам ОТО (специалистам «Казахтелеком»)». Думается, что отсутствие в постановлениях о назначении перехвата сообщений конкретных сроков связано с тем, что уголовно-процессуальный кодекс РК не регламентирует данное положение. И, таким образом, все принятые решения о производстве перехвата сообщений носили «разовый» характер.

Продолжая исследование данного вопроса, следует отметить, что «разовый» вид перехвата сообщений 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 др.).

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 тридцати суточным 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.

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 др.

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 и Закона «О прокуратуре».

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 чч. 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[1];

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 др.).

При расследовании уголовного дела в форме дознания действуют установленные выше сроки, за исключением того, что «продолжительный» срок перехвата сообщений будет ограничиваться 30-ти суточным 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 чч. 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.

---

[1] 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.

Возобновление производства перехвата сообщений производится на основании положений чч. 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».

Глава 2

ИНЫЕ МЕТОДЫ И СПОСОБЫ ОБНАРУЖЕНИЯ И ЗАКРЕПЛЕНИЯ ИНФОРМАЦИИ ПРИ ПЕРЕХВАТЕ СООБЩЕНИЙ

2.1. Файлы регистрации как источник доказательственной информации

На эффективность работы в борьбе с преступлениями в сфере высоких технологии 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»[1]. 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 преступления. 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»[1].

[1] *Сыморов Д. Н.* О последних изменениях оперативно-розыскного и уголовно-процессуального законодательства, касающихся контроля и записи телефонных и иных переговоров // Российский следователь. — 2002. — № 5. — С. 15.

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, радио-, оптической и другим электромагнитным системам связи. В специальной литературе[2] 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.

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,[3] 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

[1] *Мещеряков В. А.* Преступления в сфере компьютерной информации: правовой и криминалистический анализ. — Воронеж, 2001. — С. 74.

[2] *Вихорев С. В.* Что есть что в информационном праве. — М., 2000. — С. 9; *Ефремов А. А.* Информация как объект гражданских прав. — М., 2001. — С. 12.

[3] *Волеводз А. Г.* Следы преступлений, совершенных в компьютерных сетях // Российский следователь. — 2002. — № 1. — С. 4-54.

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 сеанса 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.

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 т. д. 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 т 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»[1].

Кроме LOG-файлов носителями доказательственной информации могут

[1] Уголовное дело № 216001 по факту неправомерного доступа в локальную сеть Актюбинского РИВЦ, возбужденное 2-м отделом 4-го Управления ДКНБ РК по Актюбинской области.

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. § 2703 (f) (2) Титула 18 Свода законов США установлено, что компетентные органы вправе получить запрашиваемые данные в течение срока их хранения, а именно на протяжении 180 дней[1].

[1] Federal Criminal Code and Rules / Title 18-- Crime and Criminal Procedure (amendmenlieceivedio February 15, 1999), West Group. St. Paul, Minn, 1999. P. 897-898.

Исследование вопроса обнаружения и фиксации следов в компьютерных сетях, позволяет сделать вывод, 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.

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.

2.2. Особенности собирания доказательственной информации при осуществлении обыска и розыска в компьютерных сетях

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[1].

В силу изложенного такая технологически возможная деятельность, по существу, превращается в самостоятельный способ обнаружения, закрепления и изъятия следов преступлений в компьютерных сетях.

---

[1] Стив Басс // Мир ПК. — 2002. — № 4. — С. 94-95.

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»[1].

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 отнюдь 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. В подобных случаях обращение за санкцией в прокуратуру крайне проблематично, поскольку отсутствуют координаты возможного местонахождения компьютерной информации.

---

[1] *Волеводз А. Г.* Следы преступлений, совершенных в компьютерных сетях // Российский следователь. — 2002. — № 1. — С. 9.

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[1]. На ее разработку и внедрение ушло несколько лет и до сих пор ведутся дискуссии о ее правомерности отлаженности действия.

Не редкость, когда искомым объектом является компьютерная информация, физическое местонахождение носителей которой не только известно, но и, по существу, не имеет какого-либо значения для следствия. В то же время имеются достаточные основания полагать, что в определенном удаленном массиве компьютерной информации на таком носителе находится требуемая, доступ к которой возможен с использованием сетевых технологий и в условиях, когда любая задержка с ее копированием может повлечь за собой ее утрату в результате действий иных лиц, а ровно иные вредные последствия[2]. В таких условиях производство выемки компьютерной информации фактически невозможно.

В настоящее время одним из решений 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.

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 Источник в электронных сетях: http://feast.ice.ru/libertarium/sorm/

2 ***Чуркин А. В.*** Проникновение следователя в жилище при помощи... компьютера (точка зрения) // Российский следователь. — 1999. — № 4. — С. 44-45.

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.

2. 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.

3. 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.

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.

2.3. Особенности и тактические приемы осмотра компьютерной техники, как объекта процессуальных действий

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 в соответствии с установленным ГОСТом.

Во-вторых, осмотр, проводимый до возбуждения уголовного дело, 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[1] «место обнаружения вещественных доказательств играет такую же роль для определения их доказательственного значения, как личность свидетеля или потерпевшего — для определения доказательственного значения их показаний». При обнаружении, «вещественный объект необходимо тщательно осмотреть, выявив все те его свойства и признаки, которые могут иметь отношение к обстоятельствам, подлежащим дока-

---

[1] *Арсеньев В. Д.* Основы теории доказательств в советском уголовном процессе. — Иркутск, 1970. — С. 82.

зыванию. Все это должно быть описано в протоколе осмотра вещественного доказательства, с обеспечением полноты и точности сведений о свойствах и признаках предмета, имеющих доказательственное значение»[1].

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 др.), похищенным имуществом, базой данных хранения различных видов информации (личной, служебной и т. п.), средством передачи и получения сообщений и др. 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 — прим. автора) целесообразно производить в форме "обысков-осмотров"»[2]. 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 путем производства осмотра, он 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[1].

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 успешно, 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,[2] а также казахстанскими[3] и российским[4] 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;

---

1 ***Горский Г. Ф., Кокорев Л. Д., Элькинд П. М.*** Проблемы доказательств в советском уголовном процессе. — Воронеж, 1978. — С. 240.

2 ***Крылов В. Б.*** Информационные компьютерные преступления. — М., 1997. — С. 74.

1 Уголовное дело № 420081201.

2 Расследование преступлений в сфере компьютерной информации: Методические рекомендации. НИЛ № 4 ВНИИ МВД РФ. — М., 1998. — С. 16.

3 ***Толеубекова Б. Х.*** Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники: Дис. … д-ра юрид. наук. — Алматы, 1998. — С. 268; ***Назмышев Р. А.*** Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. — С. 15.

4 ***Рогозин В. Ю.*** Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Дис. … канд. юрид. наук. — Волгоград, 1998. — С. 210.

– 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, т.к. 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 пр.;

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 др., шифрованных рукописных записей и пр.).

При осмотре должен присутствовать кто-либо из сотрудников предприятия, способный дать пояснения по установленному на ЭВМ программному обеспечению.

Если на начальной стадии осмотра не удалось установить пароли и коды используемых программ, то компьютер подлежит опечатыванию и выемке, с тем чтобы в последующем в стационарных условиях прокуратуры или лаборатории с привлечением специалистов-программистов 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 и работе 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 др.);

– 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 пред-

приятия; комплектацию (наличие и тип дисководов, сетевых карт, разъемов и т.д.), 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 др.);

– 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 др.) указать на возможность их подключения. Проверить их работу с исследуемым компьютером (при возникновении такой необходимости) можно в ходе следственного эксперимента[1]. Например, в ходе производства обыска по уголовному делу № 960710 по факту фальшивомонетничества, 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.

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:

1. 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.

2. 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, произошедшие изменения следует отразить в протоколе.

3. 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.

4. 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 изменять или стереть информацию.

5. 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[1]. Если возникает необходимость (и возможность), следователь может изъять информацию с ЭВМ, путем копиро-

---

[1] УПК РК — общая характеристика (в сравнении с УПК КазССР): Практическое пособие. — Алматы, 1998. — С. 280; ***Махтаев М. Ш., Соловьев Л. Н.*** Применение криминалистических методик в раскрытии и расследовании преступлений в сфере компьютерной информации: Лекция. Академия ФСБ РФ. — М., 1998. — С. 51.

[1] ***Назмышев Р. А.*** Особенности и методические проблемы расследования неправомерного доступа к компьютерной информации. — Костанай, 2000. — С. 15; ***Махтаев М. Ш., Соловьев Л. Н.*** Указ. раб. — С. 51.

вания 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.

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.

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.

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 следователем одного из райотделов. 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 +F1 — 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 «С», 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 «С», 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 т. д.)». используя данные рекомендации следователь успешно провел исследование компьютерной информации и получил необходимые сведения.

В тех же случаях, когда исследование проводилось 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 пр., чтобы можно было отличить от сходных предметов. Особо выделяются изменяющиеся признаки и особенности, которые со временем могут быть утрачены (влажность, напыление, помарки и т.д.).

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 лен-

той 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 N5126 E 0019. Произведено в декабре 1995 в Корее. Инвентарный номер отсутствует. На момент начала осмотра монитор отключен.

3. Клавиатура — FCC 1 D E 8 HKB-2313. Модель № KB-2313. Серия 5 K 83002684. На нижней панели прозрачной липкой лентой наклеен на полоске бумаги номер 01380432. К моменту начала осмотра отключена.

4. Мышь FCC 1 D E MJMU SGC. На нижней панели имеется наклейка из белой бумаги с надписью «MUSC GL V 34A AA (T6). Мышь овальной формы размером 4,5 х 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) дискет Verbatim. Один комплект копий (15 дискет) передан специалисту В. И. Головач, 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... №...».

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, 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[1]. 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 др.).
5. Тип информации, хранящейся в файле (текстовая, графическая и т. д.).
6. Машинный носитель, его тип, номер, метка и др.

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).

---

[1] *Полевой Н. С. и др.* Правовая информатика и кибернетика. — М., 1993. — С. 300; *Крылов В. Б.* Информационные компьютерные преступления. — М., 1997. — С. 235; Расследование преступлений в сфере компьютерной информации: Методические рекомендации. НИЛ № 4 ВНИИ МВД РФ. — М., 1998. — С. 22.

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 т. п.

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 № 960710, 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 MB 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»[1].

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);

[1] Уголовное дело № 960710, возбужденное СС УВД г. Петропавловска по факту фальшивомонетничества с использованием персонального компьютера.

– 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. При этом каждый из них должен быть опечатан.

– 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: «1 — 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 т.п. 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, т. к. 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 проч.).

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 из такой ЭВМ требуются специальные познания в области программирования. Осмотр компьютера в данном варианте будет только внешний, т.е. 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). 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»[1].

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.

[1] *Григорьев М. Ю.* Электронная записная книжка» как новый источник получения информации при расследовании преступлений // Российский следователь. — 1999. — № 5. — С. 41.

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 т. д.;

– 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, привлечен-

ными 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 известно 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»[1]. Принцип сохранения конфиденциальности закреплен и 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)

---

[1] 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. Сборник международных документов. — М., 1998. — С. 308.

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, под редакцией А. Н. Ахпанова, Т. Е. Сарсенбаева[1].

---

[1] Примерные образцы уголовно-процессуальных актов досудебного производства / Под общ. ред. А. Н. Ахпанова, Т. Е. Сарсенбаева. — Астана, 2000. — С. 206.

установлен в московской квартире, однако к Internety подключались через систему переадресации при помощи модемов и сотовых телефонов[1].

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 (т. е. те самые LOG-файлы). Возникшая необходимость была реализована совместным приказом 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 перезаписываемый 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[2].

Фактор времени часто имеет решающее значение при расследовании преступлений, и не случайно задачей уголовного судопроизводства ст. 8

---

1 *Силкин Л.* Как бороться с «сетевыми пиратами» // Российская юстиция. — 2002. — № 7. — С. 62.

2 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 от 20 сентября 2004 г. № 199-п «Об утверждении Правил взаимодействия государственных органов и организаций при внедрении и эксплуатации аппаратно-программных и технических средств проведения оперативно-розыскных мероприятии на сетях телекоммуникаций Республики Казахстан».

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[1].

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 *Макоренков Д. Е., Наумов И. А.* Получение информации из компьютерных систем в оперативно-розыскной деятельности правоохранительных органов // Информация правоохранительных систем: Тез. докл. междунар. конф. — М., 1999. — С. 75.

1. 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 и иных преступлений. 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.

Файлы как физические объемы, находящиеся на различных машинных носителях информации, имеют общие типичные свойства и факультативные свойства.

2. 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.

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

Во-первых, осмотр, проводимый до возбуждения уголовного дело, 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.

Во-вторых, учитывая особенности компьютерной информации, необходимо обеспечить ее обязательное документирование в соответствии с установленным ГОСТом.

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.

Следователю необходимо соблюдать отдельные тактические приемы, которые позволят недопустить утрату доказательственной информации.

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 др.);

– 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 т. д.), 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 др.);

– точно описать порядок соединения между собой указанных устройств, промаркировав (при необходимости) соединительные кабели и порты их подключения.

4. 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.

5. 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.

6. 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.

ЗАКЛЮЧЕНИЕ

В заключении хотелось бы отметить, что введение в действие, нового следственного действия — «перехват сообщений» существенного расширило сферу источников доказательств, используемых пир расследовании преступлений и изобличении виновных. В сферу уголовного судопроизводства вошли новые по природе источники доказательственной информации:

– компьютер (персональный компьютер, ЭВМ) под которым 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 т. п.) над символьной и образной информацией и через установленные каналы выходить в информационно-вычислительную сеть, а также к источникам массовой информации;

– 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 др.

В настоящем учебном пособии 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.

Так, 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 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.

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. 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 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 чч. 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 др.).

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 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.

Анализ практики реализации норм о получении информации с технических каналов связи и компьютерных систем, а также теоретическое и правовое исследование, позволили разработать рекомендации по совершенствованию законодательной регламентации применения данного вида следственного действия. Предлагается внести изменения в понятие перехвата сообщений, 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 относи-

мой 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 чч. 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 чч. 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 учреждени-

ям, 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».

В заключение хотелось бы также отметить, что, в настоящее время имеется немало возможностей, способствующих раскрытию преступлений, совершенных с использованием компьютерной техники, использованию электронной информации в качестве доказательств по уголовным делам. Однако их эффективность зависит от ряда рассмотренных объективных и субъективных обстоятельств, из которых на первое место выступает создание в системе правоохранительных органов Казахстана общего организационно-методического центра, координирующего всю работу в этом направлении, наделенного соответствующими полномочиями и способного по своему профессиональному составу заниматься всем спектром означенных в настоящей работе проблем.

КОМПЛЕКС МЕТОДИЧЕСКИХ ЗАДАНИЙ

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

ГЛАВА 1. ПЕРЕХВАТ СООБЩЕНИЙ КАК САМОСТОЯТЕЛЬНОЕ СЛЕДСТВЕННОЕ ДЕЙСТВИЕ

§ 1. Перехват сообщений как специальный процессуальный способ получения информации

- Дайте определение понятия - компьютер (персональный компьютер, ЭВМ) .
- Является ли компьютерная сеть (сеть ЭВМ) источником доказательств?
- Перечислите виды компьютерных сетей.
- Дайте определение понятия «перехват сообщений»
- Каковы основные цели и задачи перехвата сообщений?
- Что понимается под действием - «уничтожение информации»?
- Каковы условия эксплуатации ЭВМ при осуществлении блокирования информации?
- В чем заключаются действия оператора и сотрудника правоохранительных органов при модификации информации?
- Что понимается под копированием информации?
- В каких случаях производится уничтожение информации?
- В каком процессуальном документе отражаются операции, проводимые над информацией?

§ 2. Сущность и содержание перехвата сообщений

- В чем заключаются особенности производства перехвата сообщений в сравнении с обыском и прослушиванием телефонных переговоров
  - по цели
  - по объекту исследования
  - по методу проведения
  - по предмету исследования
  - по сроку действия
  - по участию специалиста
  - -- при санкционировании прокурором
- В чем заключается специфичность новой формы обыска -

электронное прослушивание и наблюдение?

- Каков порядок проведения перехвата сообщений, как следственного действия, направленного на получение информации с технических каналов связи и снятие информации с компьютерных систем?
- Что является основанием для производства перехвата сообщений?
- Дайте определение цели перехвата сообщений?
- Кто входит в состав участников проводимого действия?
- Какие органы осуществляют перехват сообщений?
- Назовите виды и сроки проведения перехвата сообщений?
- Определите порядок передачи перехваченной информации?
- Какие требования предъявляются к выносимому постановлению?
- Каковы особенности санкционирования постановления прокурором?
- Каков порядок осмотра полученной информации?
- Какие решения принимаются по перехваченной информации?

§ 3. Цели, основания и условия реализации перехвата сообщений

- В чем заключается специфичность цели перехвата сообщений?
- На что влияет точное определение цели следственного действия?
- Что относится к фактическим основаниям для перехвата сообщений?
- Каковы особенности назначения и проведения перехвата сообщений по заявлениям подозреваемых, обвиняемых и иных причастных к преступлению лицам?
- Каковы особенности назначения и проведения перехвата сообщений по заявлениям потерпевших и свидетелей??
- Как законодателем определены основания производства перехвата сообщений?
- Что является юридическим основанием для производства перехвата сообщений?
- Каковы особенности назначения и проведения перехвата сообщений по заявлениям подозреваемых, обвиняемых и иных причастных к преступлению лицам?
- Перечислите условия проведения перехвата сообщений?
- Перечислите виды участия специалиста при проведении процессуальных действий?
- В чем заключается специфичность составления постановления о производстве перехвата сообщений?

§ 4. Процессуальный порядок и сроки производства перехвата сообщений.

- Правильное исчисление процессуальных сроков является.... (разъясните).
- На что влияют ошибки в исчислении процессуальных сроков?
- Как законодателем регламентируется ограничение неприкосновенности частной жизни в области тайны сообщений, передаваемых по компьютерным и техническим каналам связи?
- В чем заключается соотношение сроков проведения следственного действия с защитой прав и интересов граждан?
- Каков порядок продления сроков перехвата сообщений?
- Чем обусловлен «продолжительный» срок перехвата сообщений?
- Разъясните основания и условия назначения «разового» срока перехвата сообщений?
- Каков порядок приостановления срока перехвата сообщений?
- В чем заключается специфичность возобновления перехвата сообщений?

ГЛАВА 2. ИНЫЕ МЕТОДЫ И СПОСОБЫ ОБНАРУЖЕНИЯ И ЗАКРЕПЛЕНИЯ ИНФОРМАЦИИ ПРИ ПЕРЕХВАТЕ СООБЩЕНИЙ.

§ 1. Файлы регистрации как источник доказательственной информации

- В чем заключаются «особенные» свойства электронной информации?
- Что понимается под «виртуальными следами»?
- Что носится к «сведениям о прохождении информации»?
- В каких файлах регистрации аккумулируются сведения о сообщениях, передаваемых по сетям электросвязи?
- Назовите две основные категории «исторических данных».
- Перечислите составляющие понятия «данные о пользователе».
- Что включают в себя «сведения о сообщении»?

§ 2 Особенности собирания доказательственной информации при осуществлении обыска и розыска в компьютерных сетях.

- В чем заключается механизм отслеживания событий на сетях электросвязи?
- Чем отличается розыск в компьютерных сетях (или в среде для

хранения компьютерных данных) с целью обнаружения и изъятия искомой компьютерной информации от обычного розыска?

- Каковы гарантии защиты конституционных прав граждан при осуществлении розыска в компьютерных сетях?
- Чем ограничены пределы розыска в компьютерных сетях?
- 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?
- В чем заключается особенности проведения СОРМ на сетях электросвязи?
- Является ли перехват сообщений разновидностью обыска в компьютерных сетях (или в среде для хранения компьютерных данных) с целью изъятия искомой компьютерной информации?
- Обязаны ли телекоммуникационные службы и Internet-провайдеры по запросу правомочных правительственных учреждений и органов принять все необходимые меры к сохранению данных или других свидетельств, имеющихся в их распоряжении?
- На каком основании «данные о сведениях» изымаются в распоряжение органов правосудия?

§ 3. Особенности и тактические приемы осмотра компьютерной техники, как объекта процессуальных действий

- Назовите цели осмотра, связанного с противоправным использованием компьютерных сетей?
- Какие обстоятельства необходимо учитывать при проведении осмотра, связанного с противоправным использованием компьютерных сетей?
- Чем обусловлено то, что «виртуальные следы» в определенных случаях не могут быть изъяты?
- Как происходит закрепление и изъятие следов компьютерных преступлений в процессуальных режимах осмотра?
- В чем заключаются особенности производства осмотра компьютера, производимого с целью обнаружения и изъятия информации интересующей следствие из памяти ЭВМ, или ее периферийных устройств?
- Возможно ли производство обыска с осуществлением осмотра компьютера?
- Каков оптимальный вариант организации и проведения осмотра

ЭВМ и машинных носителей информации?

- Какие отдельные тактические приемы необходимо соблюдать в целях недопущения утраты доказательственной информации?
- Перечислите перечень приемов по прибытии на место непосредственного действия, связанного с осмотром компьютерной техники.
- В чем заключается правильность описания в протоколе осмотра состояние наблюдаемого ЭВМ и ее аппаратных устройств во взаимосвязи между собой?
- Что может быть обнаружено в ходе поиска и изъятия информации и следов воздействия на нее вне ЭВМ?
- Что необходимо сделать, если в ходе осмотра не удалось установить пароли и коды используемых программ?
- В чем состоит сущность стадии — обследование внутрикорпусного содержания ЭВМ?
- Что является наиболее эффективным и простым способом фиксации данных из ОЗУ?
- Каковы особенности осмотра физических носителей магнитной информации?
- В чем заключаются типичные и факультативные свойства компьютерной информации, каково их доказательственное значение?
- Каков порядок и особенности изъятия и опечатывании магнитных носителей, компьютера и (или) периферийных устройств?
- В каких условиях должны осуществляться перевозка и хранение компьютерной техники?
- Какие решения принимает следователь после ознакомления с содержанием полученной в ходе осмотра компьютерной информацией?

ТЕСТОВЫЕ ЗАДАНИЯ

Чем, в соответствии с требованиями Конституции, обязан руководствоваться следователь, дознаватель в первую очередь:

A). Государственными декларациями РК;
B). Уголовно-процессуальным кодексом;
C). Законом РК "Об органах внутренних дел РК";
D). приказами и указаниями Генерального прокурора РК;
E). ведомственными приказами и указаниями.

Возможно ли производство осмотра компьютерной техники без участия понятых, с использованием научно-технических средств?

A). нет, это запрещено уголовно-процессуальным законом;
B). нет, это запрещено указанием Генерального прокурора РК;
C). нет, это запрещено постановлением Пленума Верховного Суда РК;
D). да, если нет возможности привлечь граждан в качестве понятых и, если проведение следственного действия связано с риском для их жизни и здоровья;
E). да, если понятые не желают принимать участие в следственном действии.

Вправе ли следователь заниматься специальной оперативно-розыскной деятельностью (СОРМ) по расследуемому делу:

A). да;
B). нет, следователь не вправе заниматься оперативной работой;
C). следователь вправе производить отдельные оперативно-розыскные мероприятия;
D). следователь вправе производить отдельные оперативно-поисковые мероприятия;
E). следователь вправе производить отдельные оперативно-розыскные и оперативно-поисковые мероприятия с разрешения начальника следственного подразделения.

Сколько понятых (минимальное число) должно присутствовать при производстве следственных действий, связанных с исследованием компьютерной техники:

A). достаточно одного;
B). не менее двух;
C). не менее трех;

D). не менее четырех;
E). не менее шести;

Допустимо ли при расследовании уголовного дела использование результатов СОРМ в качестве доказательств?

A). нет;
B). да, если они получены при соблюдении требований закона и используются в соответствии с положениями УПК РК;
C). да, но только в качестве ориентирующей информации;
D). да, допустимо как доказательство при любых условиях их получения;
E). да, если материалы ОРМ оформлены соответствующим образом.

Действия следователя в случае нахождения обвиняемого за пределами Республики Казахстан?

A). объявить его в розыск;
B). принять все необходимые меры к его явке;
C). заочно предъявить обвинение и дело с обвинительным заключением направить в суд;
D). направить уголовное дело для дальнейшего расследования по месту нахождения обвиняемого;
E). опубликовать в СМИ информацию о совершенном преступлении.

Сроки проведения перехвата сообщений после направления дела для производства дополнительного расследования?

A). 2 месяца;
B). 1 месяц;
C). в сроки, установленные судом либо прокурором;
D). по мере исполнения указания суда либо прокурора;
E). сроки не установлены.

Допустимо ли при производстве по уголовному делу несущественное нарушение требований Уголовно-процессуального закона:

A). недопустимо;
B). допустимо при возникновении необходимости;
C). требования могут быть нарушены, если это позволит ускорить производство расследования;

D). требования могут быть нарушены только в экстремальных ситуациях;

E). требования УПК могут быть нарушены только с санкции прокурора.

Могут ли в уголовном деле содержаться секретные материалы деятельности правоохранительных органов:

A). Нет, не могут

B). Могут, так как с материалами уголовного дела знакомится только ограниченный круг лиц

C). Могут только при наличии достоверных данных об их происхождении и при условии сохранения конфиденциальности

D). К уголовному делу могут быть приобщены только конкретные материалы, на основании которых возбуждено уголовное дело

E). Секретные материалы приобщаются к уголовному делу специальным приложением, с которым могут ознакомиться только работники правоохранительных органов

Допустимо ли в уголовном процессе использование результатов прослушивания телефонных переговоров:

A). нет;

B). допустимо, но только как ориентирующей информации;

C). допустимо, использование в качестве доказательств при условии законности их получения;

D). подобные действия грубо нарушают права граждан, и вообще не должны производиться;

E). допустимо, но только если нет других доказательств.

Решения о направлении следствия и производстве следственных действий следователь принимает:

A). самостоятельно

B). самостоятельно, за исключением случаев, когда законом предусмотрено получение санкции прокурора или решения суда

C). самостоятельно, за исключением случаев, когда законом предусмотрено утверждение начальником органа дознания

D). при предварительном согласовании с начальником следственного отдела, отделения

E). самостоятельность следователя ограничена возможностями административного воздействия со стороны руководства

Взаимодействие следователей с другими службами органов внутренних дел при расследовании преступлений осуществляется (укажите неверный вариант):

A). в соответствии с УПК

B). на основе согласованного планирования

C). на основе справедливого распределения материально-финансовых вознаграждений

D). на основе взаимного обмена информацией

E). на основе четкого разграничения компетенции каждой службы

Лицо, отвечающее за их учет и хранение электронных (компьютерных) вещественных доказательств:

A). назначается начальником отдела кадров из числа работников имеющих экономическое образование

B). назначается заместителем начальника органа внутренних дел по тылу из числа работников не имеющих коммерческих связей

C). назначается начальником органа внутренних дел из числа работников, не связанных с производством дознания и предварительного следствия

D). определяется следователем по личному усмотрению

E). за учет и хранение вещественных доказательств следователь несет персональную ответственность

Основными формами взаимодействия ОКП с другими службами МВД и другими министерствами и ведомствами являются (укажите неверный вариант):

A). проведение правового всеобуча среди населения

B). изучение материалов уголовных дел по нераскрытым преступлениям, с мест совершения которых изъяты следы и вещественные доказательства, и принятие мер к их целенаправленному использованию в раскрытии преступлений

C). участие специалистов в оперативно-розыскных мероприятиях с использованием научно-технических методов и средств

D). подготовка обзоров, информационных и методических материалов в целях внедрения в работу научных достижений, передового опыта

E). разработка совместных организационных мер по эффективному использованию криминалистических средств и методов в борьбе с преступностью

Работники ОКП привлекаются в качестве специалистов при производстве следственных действий в случаях:

A). требующих квалифицированного применения средств и методов

B). в дежурные сутки

C). определяемых, как правило, следователем или органом дознания

D). варинаты A и C

E). все варианты верны

За своевременную доставку специалиста к месту проведения следственного действия и обратно несет ответственность:

A). сам специалист

B). следователь

C). дежурный по органу

D). начальник органа дознания

E). водитель

Может ли быть привлечен для участия в осмотре компьютерной техники специалист другого отдела внутренних дел?

A). не может

B). может, в случае плохого самочувствия дежурного специалиста

C). может, при отсутствии криминалиста в штате органа внутренних дел

D). может, по указанию следователя

E). может, для обмена опытом

В случае необходимости производства следственных действий в другом районе, кто вправе их производить?

A). исключительно следователь, обслуживающий район, где необходимо произвести следственное действие

B). исключительно орган дознания, обслуживающий район, где необходимо произвести следственное действие

C). тот, у кого меньше работы

D). самостоятельно следователь, ведущий уголовное производство, либо вышеуказанные субъекты согласно отдельному поручению

E). следственные действия могут производиться лишь на территории, обслуживаемой органом уголовного преследования, в котором ведется предварительное следствие

В каком случае можно не назначать экспертизу для установления обстоятельств, имеющих значение для дела, которые могут быть получены в результате исследования материалов дела, проводимого экспертом на основе специальных научных знаний?

A). когда следователь обладает необходимыми специальными научными знаниями

B). если в практике следователя ранее проводилась экспертиза на основе аналогичной ситуации по другому уголовному делу

C). когда специалист ОКП обладает необходимыми специальными научными знаниями

D). когда очевидность обстоятельств не вызывает сомнений (к примеру, принадлежность к наркотическим средствам или исправность огнестрельного оружия)

E). нет верных вариантов

Структура заключения эксперта включает в себя (укажите неверный вариант):

A). вводной части

B). описательно-мотивировочной части

C). исследовательской части

D). диагноза

E). выводов

К документам не относится:

A). объяснения

B). справки

C). материалы, содержащие компьютерную информацию

D). видеозаписи

E). нет верного варианта

Вещественными доказательствами признаются:

A). предметы, если есть основания полагать, что они служили орудиями преступления

B). предметы, если есть основания полагать, что они сохранили на себе следы преступления

C). предметы, если есть основания полагать, что они были объектами преступных действий

D). предметы, могущие служить средствами к обнаружению преступления

E). все варианты верны

Вправе ли следователь закреплять в плане расследования по конкретному уголовному делу задачи, выполнение которых предусмотрено для иных лиц?

A). нет, так как следователь должен планировать лишь свою деятельность

B). нет, так как постановка задач для иных сотрудников является прерогативой руководства органа дознания

C). нет, так как соблюдение и выполнение плана расследования является обязанностью лишь самого следователя

D). да, так как следователь имеет право давать органам дознания обязательные для исполнения поручения, а невыполнение законных требований государственными органами, организациями, должностными лицами и гражданами влечет установленную законом ответственность

E). да, так как вмешательство в деятельность следователя влечет уголовную ответственность

СОДЕРЖАНИЕ

Учебное пособие

Сырбу Александр Владимирович

ПЕРЕХВАТ СООБЩЕНИЙ
В СИСТЕМЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Технический редактор *С. А. Айжанов*

Сдано в набор 16.10.07. Подписано в печать 19.12.07.
Усл. печ. л. 6,5. Формат $60\times84^{1}/_{16}$.
Печать офсетная. Бумага офсетная.
Тираж 500 экз. Заказ № 2009.

Тематический план издания ведомственной литературы
Карагандинского юридического института МВД РК
имени Баримбека Бейсенова на 2007 г., позиция № 11.

Отпечатано в типографии Карагандинского юридического института
МВД РК имени Баримбека Бейсенова

г. Караганда, ул. Ермекова, 124.