Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра Административного права и административной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: «Использование современных информационных телекоммуникационных систем в деятельности полиции»

Выполнил: Гатауллин Ранис Радифович
40.05.01 Правовое обеспечение национальной безопасности, год набора 2012, № 121 группа

Руководитель: кандидат социологических наук, доцент, доцент кафедры АП и АД
Курлович Павел Николавевич

Рецензент: начальник ОД ОП № 8 «Горки» по г. Казани майор полиции Платонова Людмила Валерьевна

К защите
_____
(допущена, дата)

Начальник кафедры _____

Дата защиты: "18" июля 2017 г. Оценка _____

Казань 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Центральный источник законодательства, регламентирующий деятельность полиции – Федеральный закон о полиции ставит следующие задачи, связанные с использованием современных информационно-коммуникационных технологий:

ч.3 ст.8 «Открытость и публичность» - Полиция регулярно информирует государственные и муниципальные органы, граждан о своей деятельности через средства массовой информации, информационно-телекоммуникационную сеть Интернет;

ч.5 ст.9 «Общественное доверие и поддержка граждан» - Федеральный орган исполнительной власти в сфере внутренних дел проводит постоянный мониторинг общественного мнения о деятельности полиции, а также мониторинг взаимодействия полиции с институтами гражданского общества. Результаты указанного мониторинга регулярно доводятся до сведения государственных и муниципальных органов, граждан через средства массовой информации, информационно-телекоммуникационную сеть Интернет;

ч.1 ст.11 «Использование достижений науки и техники, современных технологий и информационных систем» - Полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

ч.35 ст.13 «Права полиции» - использовать на безвозмездной основе возможности средств массовой информации и информационно-телекоммуникационной сети Интернет для размещения информации в целях установления обстоятельств совершения преступлений, лиц, их совершивших, а также для розыска лиц, скрывшихся от органов дознания, предварительного следствия или суда, и лиц, пропавших без вести.

В это связи широкое применение технологий компьютерной обработки информации в деятельности ОВД, значительно повысило эффективность ее повседневной деятельности. Применение автоматизированных рабочих мест и управляющих систем позволило снизить время реагирования на различные ситуации. Автоматизация деятельности региональных подразделений позволила сократить время на принятие управленческих решений и объединить в единую информационную систему все подразделения ОВД, находящиеся на территории региона. Используемые, в настоящее время, информационные системы позволяют автоматизировать все направления деятельности региональных подразделений ОВД, что обеспечивает оперативный обмен информацией и улучшенный доступ к информационным ресурсам.

В последние годы повышение материального и социального уровня сотрудников органов внутренних дел позволило предотвратить отток квалифицированных кадров из ведомства. Возрос уровень технической оснащенности, расширился доступ к телекоммуникационным сетям, создана мощнейшая информационно-аналитическая система обеспечения деятельности (ИСОД) МВД России, объединившая большинство подразделений. Но неправильно ставить знак тождества между функциональным развитием и качественным ростом информационно-коммуникационных процессов в правоохранительных органах. Назрела потребность в тщательном изучении вопросов использования передовых научно-технических средств при расследовании преступлений.

Появление новых средств компьютерной техники, программного обеспечения и программных продуктов открывает большие возможности по их использованию. Данные обстоятельства приводят к необходимости изучения вновь поступающих на «вооружение» компьютерных технологий и нахождения эффективных путей применения, которые состоят в совершенствовании нормативно-правовой базы и создании методов их использования. Качественное решение этих проблем позволит улучшить информационное

обеспечение деятельности сотрудников органов внутренних дел при расследовании преступлений, повысить эффективность их работы.

Проблема использования компьютерных технологий в качестве средства повышения эффективности организации правоохранительной деятельности, в частности деятельности ОВД по расследованию преступлений, в настоящее время недостаточно изучена ввиду ряда причин. Развитие компьютерных средств, информационно-телекоммуникационных систем, средств связи, возросшие возможности их применения и, как следствие, изменения в российском законодательстве привели к необходимости рассмотрения правовых, организационно-тактических и технических аспектов применения компьютерных технологий в деятельности по расследованию преступлений.

Объект изучения – общественные отношения, связанные с проблемами применения информационных технологий в деятельности полиции.

Предмет изучения – правовые нормы, организационно-правовые принципы применения телекоммуникационных систем в деятельности полиции.

Цель дипломной работы состоит в совершенствовании использования современных телекоммуникационных технологий в деятельности полиции.

Задачи дипломной работы:

- рассмотреть понятие и сущность информационных технологий,

- охарактеризовать нормативно-правовую базу регулирования информационных телекомуникационных систем,

- раскрыть особенности функционирования информационных технологий в правоохранительных органах ,

- изучить применение в деятельности сотрудников органов внутренних дел при обращении граждан информационно-телекоммуникационной технологий,

- охарактеризовать информационно-коммуникационную систему как источник следовой информацонной картины о криминальном событии,

- выявить проблемы производства отдельных следственных действий при расследовании преступлений с использованием информационно-телекоммуникационных систем.

Методологическую основу исследования составляет комплекс научных подходов, принципов и методов. Исследование опиралось на всеобщий метод познания явлений и процессов объективной действительности в их развитии и взаимообусловленности - диалектический материализм. Кроме того применялись следующие методы научных исследований: анализ и синтез, сравнительно - правовой и историко-правовой, системный, конкретно-социологический (анкетирование, интервьюирование, анализ документов, уголовных дел), формально-логический, статистический и др.; использовались фундаментальные положения общей социологии, социологии права и управления.

ГЛАВА 1. ПРАВОВЫЕ ОСНОВЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

1.1. Информационные технологии: теоретический анализ

Под информационными технологиями будем понимать систему операций по сбору, хранению, обработке и передаче правоохранительной информации с помощью компьютеров. Информационные технологии используются для обработки криминальной информации, управления, автоматизации офисных работ, принятия решений, функционирования экспертных систем.

Информационная технология является наиболее важной составляющей процесса использования информационных ресурсов общества. К настоящему времени она прошла несколько эволюционных этапов, смена которых определялась главным образом развитием научно-технического прогресса, появлением новых технических средств переработки информации. В современном обществе основным техническим средством технологии переработки ин-формации служит персональный компьютер, который существенно повлиял как на концепцию построения и использования технологических процессов, так и на качество результатной информации. Внедрение персонального компьютера в информационную сферу и применение телекоммуникационных средств связи определили новый этап развития информационной технологии и, как следствие, изменение ее названия за счет присоединения одного из синонимов: «новая», «компьютерная» или «современная».

Прилагательное «новая» подчеркивает новаторский, а не эволюционный характер этой технологии. Ее внедрение является новаторским актом в том смысле, что она существенно изменяет содержание различных видов деятельности в организациях. В понятие новой информационной технологии включены также коммуникационные технологии, которые обеспечивают

передачу информации разными средствами, а именно — телефон, телеграф, телекоммуникации, факс и др.

Правоохранительные органы - это совокупность специально уполномоченных государственных органов, которые осуществляют правоохранительную деятельность по обеспечению законности, правопорядка, охране прав и свобод человека[1].

В органах внутренних дел имеется Федеральный банк криминальной информации. В правоохранительной деятельности по своему назначению можно выделить автоматизированные информационные системы (АИС) для сбора и обработки учетной и статистической информации, оперативные, для следственной практики, криминалистические, управленческие, для экспертной деятельности.

Используются автоматизированные системы обработки данных (АСОД), автоматизированные информационно-поисковые системы (АИПС), автоматизированные информационно-справочные системы (АИСС), автоматизированные рабочие места (АРМ), автоматизированные системы управления (АСУ), экспертные системы. Возможны и комбинации этих АИС.

АСОД обычно применяются для выполнения относительно несложных, стандартных операций с данными, автоматизируют работу персонала невысокой квалификации. АИПС служат для поиска, отбора, выдачи правовой и криминалистической информации по запросам, оформленным соответствующим образом; бывают документальные и фактографические. АИСС выдают справки по вопросам правоохраны и правопорядка по запросам без сложного преобразования данных.

Так АИСС «Сводка» выдает справки о происшествиях преступлениях по оперативной информации.

АИСС «Гастролеры» выдает справки о преступлениях на транспорте, не разысканных вещах, подозрительных лицах и их связях; с использованием ППП

[1] Гуценко К.Ф., Ковалев М.А. Правоохранительные органы. Учебник для юридических вузов и факультетов. Изд. 8-е,перераб. и доп/Под ред. К.Ф. Гуценко. М.: Издательство Зеркало-М,2016.-416.

«Flint» может решать поисковые задачи типа «лицо», «нераскрытые преступления», «вещи».

АИСС «Грузы-ЖД» снабжает справками о хищениях груза и багажа на железных дорогах.

АИСС «Наркобизнес» предоставляет справки по криминальному обороту наркотиков.

АИСС «Картотека-Регион» с использованием СУБД «Adabas» выдает фамилии, имена, отчества осужденных, разыскиваемых лиц, бродяг, задержанных; может распределять места отбытия наказания, решать административные задачи по осужденным лицам.

АИСС «Спецаппарат» предназначена для работы со спецаппаратом и поиска информации по спецсообщениям (поиск лиц по однотипным преступлениям и способам совершения, по адресам и т.п.) [2].

Автоматизированное рабочее место (АРМ) представляет собой комплекс технических и программных средств для автоматизации профессиональной деятельности.

В типовой состав АРМ входят персональный компьютер, принтер, плоттер, сканер, факс, средства сетевой связи и другие устройства, а из программных средств – текстовый процессор, электронные таблицы, графические процессоры, офисные приложения. Пол иногда понимают рабочие места, а иногда – ППП[3].

Существуют три типа АРМ:

1) индивидуального пользования,

2) группового пользования,

3) сетевые.

Сетевые АРМ представляются наиболее перспективными, так как позволяют связываться с удаленными банками данных и обмениваться

---

[2]Логиновский О.В., Максимов А.А. Основные положения решения задач информатизации правоохранительных органов// Международные системы – 2015.-№ 4.

[3] Кирин В.И., Минаев В.А. Информатика в деятельности органов внутренних дел: Учеб. пособие. М., 2011.

информацией между различными подразделениями правоохранительных органов. Примером может служить АРМ «ГРОВД» для городских и районных отделов внутренних дел.

АСУ представляют собой комплексы технических и программных средств для автоматизированного управления различными службами и органами правоохраны.

Основная функция таких АСУ – обеспечение руководителей служебной информацией. Практически это система связанных АРМ. Примером может служить АСУ «Дежурная часть» (АСУ ДЧ), предназначенная для управления силами и средствами ОВД в оперативной работе[4].

Основные функции АСУ:

1) Оперативный сбор и анализ оперативной информации, выдача указаний подразделениям ОВД, контроль за выполнением оперативной работы в реальном масштабе времени, управление подвижными милицейскими группами (на автомобилях, мотоциклах и других моторизованных средствах передвижения).

2) Сбор, обработка, хранение информации; отображение информации о размещении сил и средств, а также о местах совершения преступлений на фоне представленных на экране («электронных») карт.

3) Сбор информации о правонарушителях, похищенных вещах и транспортных средствах; выдача информации по запросам органов внутренних дел с использованием банков данных.

4) Регистрация деятельности органов внутренних дел, подготовка отчетов о работе, анализ процессов (событий).

Использование АСУ позволяет радикально упростить и ускорить выполнение указанных работ.

Обособленной разновидностью информации следует считать информацию, размещенную в глобальной сети Интернет. Там применяются

[4]Логиновский О.В., Максимов А.А. Основные положения решения задач информатизации правоохранительных органов// Международные системы – 2010.-№ 4.

специфические приемы поиска, обработки, хранения и передачи распределенной информации значительных объемов и способы работы с разнообразными видами информации. Непрерывно развивается программное обеспечение, делающее возможным коллективный доступ к информации всех видов.

Главная особенность Интернета – разработка стандартов программного обеспечения для межсетевой связи, которым дали название TCP, а позже TCP/IP – Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Межсетевой протокол). Создатели реализовали программное обеспечение, с помощью которого данные всех типов «упаковываются» и в упакованном виде пересылаются из сети в сеть. В сети получателя данные «распаковываются», и на экране компьютера возникают тексты, цифры и графики. Лучшая аналогия TCP/IP – контейнерная перевозка. Содержание контейнеров не играет роли, но все контейнеры имеют одинаковые габариты. Их можно перевозить на любом виде транспорта и легко перегружать с одного транспортного средства на следующее. TCP/IP определяет габариты «контейнера с данными», межсетевой компьютер «перегружает» контейнеры[5].

Учитывая повсеместное проникновение информационных технологий, законодатель не мог оставаться в стороне от разработки соответствующих норм и понятий. Так, им определено, что информационные правоотношения – это отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, поиска, распространения и представления потребителю документированной информации; создании, использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации. Информационный процесс – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

[5]Грошиков В. А. Использование информационных технологий в раскрытии тяжких преступлений / В. А. Грошиков // Вестник Волгоградской академии МВД России. – 2014. – № 1. – С. 39-42.

Несколько лет назад, перед Министерством внутренних дел Российской Федерации, в связи с использованием передовых технологий, возникла проблема взаимодействия всех структурных подразделений МВД на территории нашей страны. Требовалось создать единый сервис для организации централизованного хранения и обработки данных. Эта система должна была стать единым источником информации для всех сотрудников подразделений МВД, служить для организации электронного взаимодействия между ними, обеспечения разграниченного доступа к информационным ресурсам. Проблема оставалась довольно актуальной, поэтому в марте 2012 года была утверждена концепция создания ИСОД[6].

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) органов внутренних дел, который разрабатывался с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений органов внутренних дел с другими правоохранительными органами и государственными органами различных уровней.

Для решения проблемы доступа к информационным ресурсам Министерством внутренних дел Российской Федерации были приняты следующие приказы:

1) Приказ МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры»[7].

---

[6] Леднев К. Ю. ИСОД МВД России и основной элемент инфраструктуры – ЕИС ЦОД // Информационные технологии, связь и защита информации МВД России. 2012. № 1. С. 25–27.

[7] Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры» [Электронный ресурс]: Приказ МВД России от 16 января 2012 г. № 25. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

2) Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации»[8].

ИСОД МВД России представляет собой совокупность средств вычислительной техники, телекоммуникационного оборудования, а также содержащейся в базах данных информации, обрабатываемой с использованием информационных технологий в интересах МВД России. ИСОД МВД России направлена на развитие и совершенствование технологий и функций автоматизации и информатизации МВД России, заложенных в Единой информационно-телекоммуникационной системе органов внутренних дел (ЕИТКС ОВД).

Основным элементом инфраструктуры ИСОД МВД является Единая информационная система централизованной обработки данных (ЕИС ЦОД), которая создается на нескольких территориально удаленных площадках. Она предназначена для размещения централизованных информационных систем и сервисов МВД России и предоставления доступа к ним с использованием облачных технологий. За счет создания ЕИС ЦОД унифицированы используемые в органах внутренних дел программно-технические решения и приведена архитектура основных автоматизированных информационных систем в соответствие современным требованиям к доступности и надежности информационных ресурсов.

Данная информационная система обеспечила консолидацию разнородных данных, содержащихся в различных системах МВД и обеспечила единую точку доступа к ним для использования в оперативно-служебной деятельности МВД России. Интегрированная система обработки данных предусматривает замену разрозненных справочников, каталогов и картотек единой формой организации всех сведений многократного использования. Поскольку интегрированная система обработки данных представляет собой единую систему,

[8] Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: Приказ МВД России от 6 июля 2012 г. № 678 // Рос. газ. 2012. 5 окт. № 230.

обрабатывающую информацию совместно по всем функциям управления и распределяющую эту информацию функциональным подразделениям, через нее проходит и информация о решениях, принятых специалистами. Практически любое экономическое решение по одной функции затрагивает многие другие функции. Согласование решений по различным функциям осуществляется интегрированной системой путем передачи соответствующей информации заинтересованным подразделениям.

В состав ИСОД МВД России входят следующие компоненты:

1) облачная инфраструктура, состоящая из совокупности вычислительных средств обработки информации, средств хранения информации, расположенных в центрах обработки данных (ЦОД ИСОД МВД России), и программно-технических комплексов единого информационного пространства (ПТК);

2) сервисы ИСОД МВД России — программные информационные сервисы, функционирующие на базе облачной инфраструктуры и обеспечивающие выполнение служебно-оперативной деятельности сотрудников МВД России, выполнение государственных услуг и функций ведения централизованных банков данных МВД России;

3) интегрированная мульти сервисная телекоммуникационная система (ИМТС);

4) автоматизированные рабочие места (АРМ) сотрудников МВД.

ИСОД МВД России обеспечивает реализацию следующих основных функций:

- автоматизация прикладных функций ведомственных общесистемных сервисов, а также сервисов оперативно-служебной деятельности;

- хранение и обработка данных ведомственных централизованных банков данных;

- комплексный анализ данных ведомственных централизованных банков данных;

- разграничение доступа к ресурсам ИСОД МВД России.

Подводя итог, необходимо отметить, что в процессе создания ИСОД были решены задачи автоматизации основных видов деятельности подразделений МВД, организации централизованного хранения и обработки данных. Сотрудники полиции получили возможность более быстрого доступа к требуемой информации. Были снижены трудозатраты на получение, обработку, хранение информации и доведение ее до пользователей. Именно Единая система информационно-аналитического обеспечения дала возможность системного подхода к внедрению автоматизированных систем в органах внутренних дел.

1.2 Нормативно-правовая база регулирования информационных телекоммуникационных систем

Современные информационные процессы представляют собой одну из наиболее важных составляющих социальной, экономической и политической деятельности человека и общества. Ключевую роль в развитии современного общества играют информационные технологии, без использования которых стала немыслимой деятельность и функционирование важнейших институтов человеческой цивилизации.

В настоящий момент уже можно с уверенность утверждать, что человечество вступило в новую фазу своего развития – фазу так называемого «информационного общества». Не осталась в стороне от этих процессов и Россия, где бурное развитие информационных технологий (ИТ) на рубеже веков стремительно превратило российское общество в информационное. Проникновение информационных технологий во все без исключения сферы деятельности российского государства обусловило необходимость легального определения этого феномена. Впервые понятие «информационного общества» получило легальное определение в «Стратегии развития информационного общества в России»[9]. Этот документ задал концептуальную и стратегическую

[9] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212). – Режим доступа: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html.

цель для дальнейшего движения к информационному обществу и развития информационного права.

Стратегия выступает «основой для подготовки и уточнения доктринальных, концептуальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, а также принципы и механизмы их взаимодействия с организациями и гражданами в области развития информационного общества в Российской Федерации»[10]. Благодаря ее реализации Россия должна войти в двадцатку лидеров глобального информационного общества, а по показателю доступности информационной и телекоммуникационной инфраструктуры для граждан и организаций – в десятку стран-лидеров.

Стратегией развития информационного общества в России закрепляются принципы государственной политики в сфере информатизации, а именно:

- партнерство государства, бизнеса и гражданского общества;

- свобода и равенство доступа к информации и знаниям;

- поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;

- содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;

- обеспечение национальной безопасности в информационной сфере.

Суть Стратегии развития информационного общества в России состоит в том, что государство гарантирует обществу создание таких условий, при которых любой гражданин сможет максимально эффективно пользоваться информационно-коммуникационными технологиями, в том числе для доступа к информации о деятельности органов власти, получения государственных и муниципальных услуг в электронном формате и защиты своих прав.

[10] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212). – Режим доступа: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html.

Определены основные направления деятельности органов власти по реализации Стратегии развития информационного общества в России, частности:

- разработка перечня нормативных правовых актов, направленных на регулирование вопросов оказания государственных и муниципальных услуг, в том числе вопросов оказания таких услуг в электронном виде;

- завершение формирования единой информационно-технологической и телекоммуникационной инфраструктуры электронного правительства;

- создание единого портала государственных и муниципальных услуг;

- переход на электронный документооборот;

- информатизация процесса аттестации, подготовки и повышения квалификации государственных и муниципальных служащих, работников бюджетной сферы;

- ликвидация цифрового разрыва, обучение населения основам компьютерной грамотности и др.

Необходимо отметить, что формирование правовой базы информационного общества в России началось еще в прошлом веке и продолжается в настоящее время. Этот процесс непрерывный, поскольку специфика информационного общества в том и заключается, что его изменение происходит со все возрастающей скоростью. В то время как процесс принятия законов занимает достаточно большой промежуток времени.

В настоящий момент правовую базу информационного общества в нашей стране составляет целый ряд законодательных и нормативно-правовых актов, позволяющих говорить о самостоятельной отрасли российского законодательства – отрасли информационного права[11].

Именно этот сегмент российской правовой системы призван создать основы правового регулирования в области информационных технологий, хранения, распространения и защиты информации. Базовым законодательным

[11] Тедеев, А.А. Проблемы и условия правового регулирования интернет-отношений / А.А. Тедеев // Информационное право. – 2014. – № 4. – С.87.

актом в области информационного права является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[12]. Этим Законом регулируются отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Одним из важных условий формирования и функционирования информационного общества в нашей стране является реализация основных положений Федерального закона от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Этот Закон впервые законодательно определил основные способы доступа к информации о деятельности органов государственной власти и местного самоуправления, включая доступ в электронном формате. Закрепил состав информации о деятельности государственных органов и органов местного самоуправления, размещаемой в сети Интернет (иными словами, законодательно был закреплен статус официальных сайтов органов власти как инструмента взаимодействия с населением). Кроме того, Закон закрепил процедуру подачи запроса о получении информации и ответа на него:

- требования к запросу о получении информации,
- сроки и порядок рассмотрения запроса,
- требования к ответу на запрос,
- основания для отказа в предоставлении информации.

Наряду с Федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» свой вклад в формирование правовой базы реализации Стратегии развития информационного общества в России внесли:

---

[12] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 21.07.2014) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

- Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»;

- Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

- Закон РФ от 27.12.1991 N 2124-1 (ред. от 28.07.2012) «О средствах массовой информации»;

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

- Федеральный закон от 27.07.2010 № 224-ФЗ (ред. от 11.07.2011) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».

Кроме того, был принят целый ряд подзаконных нормативно-правовых актов: указов, постановлений и распоряжений, направленных на реализацию вышеуказанных нормативных документов и на повышение качества государственной политики в сфере движения к информационному обществу на всех уровнях власти, в том числе:

- Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России»,

- Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации[13],

- Приказ МВД РФ от 14.03.2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года»[14],

- Приказ МВД РФ от 28 июня 2013 г. № 490 «Об утверждении Перечня информации о деятельности образовательных организаций системы МВД

---

[13] Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации: приказ МВД России от 12.09.2013 г. №707 (в ред. от 20.04.2015) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

[14] Приказ МВД РФ от 14.03.2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» / http://policemagazine.ru/forum/showthread.php?t=3663.

России для размещения в открытых информационно-телекоммуникационных сетях, в том числе на официальном сайте МВД России в информационно-телекоммуникационной сети «Интернет», а также Порядка размещения этой информации»[15],

- Приказ Федеральной службы по надзору в сфере образования и науки от 29 мая 2014 г. № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации»[16],

- Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры»[17],

- Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации[18],

- и т. д.

В заключение хотелось бы отметить, что реализация Стратегии развития информационного общества в России требует дальнейшего совершенствования существующей нормативно-правовой базы. В научной литературе все чаще высказывается мысль, что нормативно-правовое регулирование

---

[15] Приказ МВД РФ от 28 июня 2013 г. № 490 «Об утверждении Перечня информации о деятельности образовательных организаций системы МВД России для размещения в открытых информационно-телекоммуникационных сетях, в том числе на официальном сайте МВД России в информационно-телекоммуникационной сети «Интернет», а также Порядка размещения этой информации». http://www.garant.ru/products/ipo/prime/doc/70359132/

[16] Приказ Федеральной службы по надзору в сфере образования и науки от 29 мая 2014 г. № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации». http://www.rg.ru/2014/08/21/rosobrnadzor-dok.html

[17]Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры» [Электронный ресурс]: Приказ МВД России от 16 января 2012 г. № 25. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

[18] Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: Приказ МВД России от 6 июля 2012 г. № 678 // Рос. газ. 2012. 5 окт. № 230.

информационных отношений может вызвать необходимость их кодификации и принятия Информационного кодекса Российской Федерации[19].

[19] Тедеев, А.А. Проблемы и условия правового регулирования интернет-отношений / А.А. Тедеев // Информационное право. – 2014. – № 4. – С.87.

ГЛАВА 2. ОРГАНИЗАЦИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

2.1 Функционирование информационных технологий в правоохранительных органах

Важнейшее значение техники – способность существенно повышать эффективность труда человека посредством фрагментарной или полной замены его производительных функций. Техника (вместе с людьми, ее создающими и приводящими в действие) образует составную часть производительных сил общества и является показателем тех общественных отношений, при которых совершается труд. Термин «технические средства» широко применяется в различных сферах практической деятельности: образовании, автоматизации производства, медицинской диагностики и т. п. Становление и прогресс техники и ее средств первоначально имели место на эмпирическом уровне. Но во второй половине XIX в. происходит проникновение науки в производственную сферу, все более развивающуюся по мере совершенствования науки и техники. Увеличивается составляющая науки в разработке и применении техники и технических средств. Как следствие, на текущем историческом этапе наука существует как автономная область знания и как самостоятельная производительная сила, являющаяся неотъемлемым компонентом научно-технического прогресса[20].

При неуклонно возрастающих возможностях отечественной науки и индустрии на первый план выходит правильное определение вектора развития профильных научных разработок, в том числе в области ТКО. В качестве теоретической базы для этого можно использовать методику А. Ф. Волынского, который предлагает при решении подобных задач анализировать следующие массивы данных:

[20] Казначей И. В. Особенности использования технических средств коммуникации при производстве оперативно-разыскных мероприятий / И. В. Казначей // Вестник Волгоградской академии МВД России. – 2013. – № 4. - С. 59-63.

– криминальные динамику и структуру (данные статистической отчетности, выводы криминологического анализа);

– актуальность (повторяемость) технико-криминалистических задач и результативность их решения;

– уровень оснащенности правоохранительных органов техническими новинками, их потребности в обновлении и совершенствовании имеющихся технико-криминалистических средств;

– уровень технической оснащенности полиции передовых зарубежных стран;

– новейшие достижения естественных и технических отраслей науки, которые могут быть интегрированы в процесс разработки методов и средств криминалистической техники.

Уже сегодня теоретики и практики законотворческой и правоприменительной деятельности предвидят актуальность оперативной нормативной регламентации использования таких новейших технических разработок, как тензометрическая платформа диагностирования стрессового состояния человека, системы для ведения «электронных» уголовных дел, «электронный судья», видеопротоколы, видеоконференц-связь (видеосвязь) и др. Адекватное понимание сущности и форм ТКО, позволяет анализировать и определять перспективные направления для увеличения эффективности правоохранительной деятельности в целом и ТКО в частности как ее элемента.

Важнейшее преобразование, которое мы стремимся осуществить, – использование информационно-коммуникационных технологий. Как следствие, необходимо обратить пристальное внимание на те разновидности ИКТ, которые подлежат применению при расследовании преступлений.

Видеоконференция – область информационной технологии, обеспечивающая одновременно двустороннюю передачу, обработку, преобразование и представление интерактивной информации на расстояние в режиме реального времени с помощью аппаратно-программных средств вычислительной техники. Взаимодействие в режиме видеоконференций также

называют сеансом видеоконференц-связи. Видеоконференция применяется как средство оперативного принятия решения при чрезвычайных ситуациях, для сокращения командировочных расходов в территориально распределенных организациях, повышения эффективности, проведения судебных процессов с дистанционным участием осужденных, а также как один из элементов технологий дистанционного обучения и проч.[21]

Видеоконференц-связь – это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном масштабе времени с учетом передачи управляющих данных.

Для общения в режиме видеоконференции абонент должен иметь терминальное устройство (кодек) видеоконференц-связи, видеотелефон или иное средство вычислительной техники. Как правило, в комплекс устройств для видеоконференц-связи входит: – центральное устройство – кодек с видеокамерой и микрофоном, обеспечивающее кодирование/декодирование аудио- и видеоинформации, захват и отображение контента (информационного содержимого); – устройство передачи информации (например, модем); – устройство отображения информации и воспроизведения звука. В качестве кодека может использоваться персональный компьютер с программным обеспечением для видеоконференций.

Преимущества программных средств ВКС:

– возможность обновлений без необходимости замены аппаратной части;

– не требуют значительных вложений в инфраструктуру;

– нет необходимости в дополнительном оборудовании для реализации полного спектра возможностей (запись, совместная работа и т. п.);

– приспособлены для работы на нестабильных каналах связи, таких как Интернет.

---

[21] Лавров В.П. К вопросу о соотношении криминалистики и организации расследования преступлений / В.П. Лавров // В сборнике: Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью Всероссийская научно-практическая конференция. - Орловский юридический институт МВД России имени В.В. Лукьянова; Редколлегия: А.В. Булыжкин и др.. 2015. - С. 226-232.

Транспортная сеть передачи данных (каналы связи) играет важнейшую роль в организации видеоконференции. Сетевые протоколы IP или ISDN используются для подключения к каналам связи. Информационно-телекоммуникационная сеть Интернет – простейший и наиболее дешевый способ организации видеоконференц-связи. При этом Интернет при передаче аудио- и видеоданных не принято считать гарантированным каналом. Довольно низким может быть в данном случае качество сеанса связи. К этому добавляется проблема безопасности видеоконференции. Именно из этих соображений в МВД России введён запрет на использование Интернет для организации служебных сеансов видеоконференц-связи. Но это далеко не единственный канал, даже не самый распространенный.

Представляется, что в большей мере приближено, однако не вполне соответствует правовым и практическим реалиям определение видеоконференц-связи, предлагаемое В. И. Решетняк: это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в режиме реального времени с учетом передачи управляющих данных[22].

В ст. 11 УПК РФ предусматривается охрана в уголовном судопроизводстве прав и свобод человека и гражданина, но закон не в силах учесть современных возможностей информационно-телекоммуникационных систем и развитие информационной сферы уголовного процесса.

Исключение доступа случайных пользователей или злоумышленников выгодно отличает технологию VPN от остальных. Зависимость от иностранных производителей компьютерной техники может представлять серьезную угрозу государственным интересам. Коллегией МВД России принят ряд решений, направленных на постепенный отказ от иностранного программного обеспечения.

---

[22] Решетняк В. И. Видеоконференц-связь в судебных стадиях уголовного судопроизводства // Перспективы развития уголовно- процессуального права и криминалистики: материалы II междунар.-практ. конф., Москва, 11–12 апреля 2012 г. М., 2012. С.11-15.

Прогнозируема перспектива создания межведомственной структуры, которая могла бы отвечать нуждам всех органов предварительного расследования, независимо от принадлежности к той или иной структуре системы обеспечения правопорядка. Однако мы в настоящее время обладаем данными, позволяющими оценить потребность в такого рода преобразованиях только применительно к МВД России.

В ОВД роль специалистов должны будут играть сотрудники подразделений (отделов или групп) информационного обеспечения. Вопрос о специализации отдельных сотрудников на обеспечении производства видеоконференций актуален, ведь подобный навык необходим не только при производстве следственных действий, но для использования коммуникативных сегментов ИСОД МВД России. Данные специалисты должны будут пройти первоначальную подготовку по изучению возможностей оборудования, которым им предстоит пользоваться во время сеансов видеоконференц-связи, функций программного обеспечения, свойств каналов связи. Следует предусмотреть полноценное методическое обеспечение этой работы: разработку учебных и справочных материалов, проведение семинаров, многоступенчатую систему повышения квалификации.

Как отмечает В. Б. Вехов, изменения, свершившиеся благодаря техническому прогрессу, столь обширны, что предопределяют следующие векторы развития процессуального законодательства:

– расширение пределов допустимости и появление новых источников фактических данных;

– расширение перечня традиционных следственных действий, разработка дополнительных гарантий соблюдения законности при их производстве;

– использование компьютерных систем при принятии процессуально значимых решений.

Среди наиболее перспективных направлений развития ТКО им выделено использование компьютерной информации (в том числе электронных документов) в качестве доказательств.

Предпочтительной является форма видеоконференц-связи (далее по тексту - ВКС) применительно, прежде всего, к таким следственным действиям, как допрос, очная ставка, предъявление для опознания и освидетельствование. Оговоримся, что ограничиться четырьмя следственными действиями мы предлагаем именно на современном этапе, отталкиваясь от представлений о реалистичности постановки задач и научного прогнозирования. Перечисленные следственные действия имеют высокий коэффициент повторяемости в правоприменительной практике. Для проведения допроса, очной ставки, предъявления для опознания и освидетельствования достаточно стационарных помещений для ВКС со стандартными техническими настройками и требованиями к связи.

Существует возможность избежать очень многих случаев этапирования к месту проведения предварительного расследования лиц, содержащихся в исправительных учреждениях и следственных изоляторах. Причем в данной ситуации возникает потребность в информационно-коммуникационных технологиях на стадии производства проверочных мероприятий. Ведь при необходимости получения от осужденного показаний о преступной деятельности других лиц в целях изобличения последних (допрос, очная ставка, предъявление лица для опознания) будет достаточно доставить лицо, содержащееся в пенитенциарном учреждении, в местный орган внутренних дел.

ИКТ способны комплексно решать проблемы расследования преступлений: снижать его стоимость, сокращать сроки производства по уголовным делам (параллельно увеличивая возможность расследовать их одновременно и в большем количестве, и с достижением более высокого качества), обеспечивать на более высоком уровне безопасность участников процесса. Новизна исследуемой проблематики предполагает создание новой методики использования компьютерной техники в процессе обеспечения расследования преступлений путем анализа применяемых, внедряемых и

подлежащих внедрению методов расследования по уголовным делам[23].

Критериями допустимости применения методов, в том числе и в области информационных технологий в криминалистике, выступают:

- законность,
- этичность,
- эффективность,
- безопасность,
- обоснованность,
- экономичность[24].

Относительно допустимости метода использования средств информационно-компьютерного обеспечения при расследовании преступления критерием станет их соответствие уровню развития современных коммуникационных технологий. Выраженное значение имеет также уровень специальной подготовки субъектов, в прямой зависимости от которого находится время и качество получаемого результата работы информационной системы. Важнейшим требованием к исследуемым методам становится и эффективность: они должны создавать условия для оперативного решения проблемы с оптимальной функциональной отдачей. Многие из существующих на сегодняшний день методов реализуются в АИПС либо экспертных системах профильного назначения. Например, при диагностике изображений разверток следов выстрела, снятых с помощью комплекса «ТАИС-3» применяют метод наблюдения и сравнения через соотношение фрагментов изображений в цифровом варианте. В АДИС «Папилон», например, используются методы сравнения, наложения, измерения, совмещения при выборке рекомендательных списков из обширного массива дактилокарт вариантов, сходных по строению линий обнаруженных папиллярных узоров.

Специальные программы, разработанные для сотрудников следственных

---

[23] Казначей И. В. Особенности использования технических средств коммуникации при производстве оперативно-разыскных мероприятий / И. В. Казначей // Вестник Волгоградской академии МВД России. – 2013. – № 4. - С. 59-63.

[24]Грошиков В. А. Использование информационных технологий в раскрытии тяжких преступлений / В. А. Грошиков // Вестник Волгоградской академии МВД России. – 2014. – № 1. – С. 39-42.

аппаратов («Бинар-3», «СПРУТ» и др.), посредством моделирования помогают выдвинуть версию события, а на основе метода сравнения аналогичных следственных ситуаций запланировать направления расследования. В Следственном департаменте МВД России использование АИПС «Бинар-3» способствовало резкому сокращению временных затрат на составление обвинительных заключений по чрезвычайно сложным и объемным уголовным делам.

ИКТ и сегодня используются правоохранительными органами в их профессиональной деятельности. Уже упоминавшаяся нами ведомственная ИСОД, например, активно применяется для проведения служебных совещаний. Она содержит множество информационных сегментов, открывающих доступ к обширной базе самых разнообразных сведений, в том числе к оперативным, справочным и криминалистическим централизованным учетам. Распространена также практика оборудования отдельных подразделений локальными компьютерными сетями, что облегчает циркуляцию служебной информации внутри них.

Кроме того, почти повсеместно сегодня применяются электронная почта, IP-телефония и факсимильная связь. Необходимо отметить, что далеко не все приведенные способы использования ИКТ можно охарактеризовать как технико-криминалистические, поскольку информация, поступающая посредством таких каналов, относится к категории ориентирующей. На сегодняшний день ИКТ для обнаружения и фиксации доказательств не применяются.

На сегодняшний день методика использования информационных технологий при расследовании преступлений должна базироваться на следующих компонентах:

– сегментирование отдельных следственных действий (их этапов – подготовка, проведение, фиксация хода и результатов) на базе повсеместного использования информационных технологий на каждом из таких этапов.

Варианты решений здесь разнообразны: от электронных записных

книжек и органайзеров до применения интегрированных компьютерных систем, организующих последовательность проведения следственных действий и оперативных мероприятий, а также другие процессуальные или методические функции в расследовании уголовных дел;

– осуществление программного сопровождения уголовного процесса на всех его стадиях.

При этом можно выделить следующие перспективы применения ИКТ при организации и производстве следственных и процессуальных действий:

– технология видеоконференц-связи – может составить научно-техническую основу дистанционного проведения ряда следственных действий (допроса, очной ставки, предъявления для опознания, освидетельствования);

– электронная почта – может применяться для организации ознакомления участников расследования с материалами уголовного дела в необходимом объеме; для направления заявлений, жалоб, ходатайств в адрес следователя (руководителя следственного органа) и последующего уведомления о результатах их рассмотрения; для обеспечения явки участников к следователю;

– IP-телефония – может применяться для получения следователем консультации специалиста на предмет постановки вопросов эксперту; для обеспечения права подозреваемого или обвиняемого на получение услуг защитника. Отсюда следует вывод, что представленные достижения в области информационных средств, подлежащих внедрению в процесс расследования преступлений, на современном этапе их развития предопределили разработку методологии системного и единообразного применения ИКТ как одного из перспективных направлений криминалистической техники.

Итак, ключевыми современными проблемами ТКО являются:

- порядок использования вновь разрабатываемых научно-технических средств в уголовном судопроизводстве;

- определение вектора развития профильных научных разработок;

- увеличение потенциальной возможности удовлетворения как можно большего количества «заявок на обслуживание»;

- снижение стоимости расследования;

- сокращение длительности расследования;

- исключение вероятности осуждения невинных и оправдания преступников;

- обеспечение безопасности участников расследования[25].

Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений – это нормативно урегулированная система научно обоснованных и безопасных средств и методов, которые обеспечивают субъекту доказывания возможность дистанционного обнаружения, сбора, хранения, передачи и использования доказательственной и ориентирующей криминалистически значимой информации.

2.2. Использование сотрудниками органов внутренних дел информационно-телекоммуникационных технологий при рассмотрении обращении граждан

Основными целями осуществляемой в России в последнее десятилетие административной реформы являются повышение качества жизни наших граждан, устойчивое развитие всего общества, сокращение расходов на содержание органов государственной власти при росте эффективности их деятельности.

Цель – сокращение расходов на административный аппарат – может быть достигнута только сокращением числа работников этой сферы. Однако без изменений методики работы, без внедрения в деятельность органов государственной власти информационно- телекоммуникационных технологий, существенно повышающих качество оказываемых публичных услуг, облегчающих доступ к ним граждан, исключающих человеческий (в том числе

[25] Лавров В.П. К вопросу о соотношении криминалистики и организации расследования преступлений / В.П. Лавров // В сборнике: Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью Всероссийская научно-практическая конференция. - Орловский юридический институт МВД России имени В.В. Лукьянова; Редколлегия: А.В. Булыжкин и др.. 2015. - С. 226-232.

и коррупциогенный) фактор из данной цепочки, желаемый результат вряд ли будет получен.

Количественное сокращение госаппарата должно сопровождаться технологическими изменениями в работе госорганов. А это возможно путем перевода государственных и муниципальных услуг в электронную форму и их предоставления с использованием информационно-телекоммуникационной технологии.

Первым шагом к внедрению информационно- телекоммуникационной технологии в жизнь нашего общества стало появление в России многофункциональных центров. Как отметил председатель Правительства Российской Федерации Д.А. Медведев «многофункциональные центры по предоставлению государственных и муниципальных услуг – это линия прямого соприкосновения государства и наших граждан… Государство должно сделать все, чтобы стать для наших людей более дружелюбным, открытым, эффективным и, конечно, оперативным»[26].

Государственные и муниципальные услуги – явление достаточно новое для Российской Федерации и ее регионов. Определение этих услуг содержится в Федеральном законе №210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Государственная услуга, предоставляемая федеральным органом исполнительной власти, органом государственного внебюджетного фонда, исполнительным органом государственной власти субъекта Российской Федерации, а также органом местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации, – это деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти

[26] Из текста выступления Председателя правительства Российской Федерации Д.А. Медведева по итогам совещания «О развитии сети многофункциональных центров по предоставлению государственных и муниципальных услуг», состоявшегося 18 января 2013 г. [Электронный ресурс]. http://www.government.ru (дата обращения: 20.08.2015)

субъекта Российской Федерации, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации, которая осуществляется по запросам заявителей в пределах установленных нормативными правовыми актами Российской Федерации и нормативными правовыми актами субъектов Российской Федерации полномо- чий органов, предоставляющих государственные услуги[27].

Очередным этапом реализации государственных и муниципальных услуг населению в России стал запуск проекта «Электронное правительство». Необходимость сориентировать данный проект на нужды и запросы граждан, максимально полно раскрыть информацию о деятельности органов государственной и муниципальной власти подчеркнул Президент Российской Федерации В.В. Путин в своей статье «Демократия и качество государства»[28]. Глава государства отметил важность перехода к стандартам государственных и муниципальных услуг нового поколения, основанным не на позиции исполнителя, а на позиции потребителя этих услуг. Закономерной реакцией руководства страны на потребность российского общества в повышении доверия к органам внутренних дел и качественном улучшении их деятельности стали преобразования в МВД России[29].

Стоит сказать, что не всегда удавалось соблюсти баланс сокращения расходов на административный аппарат и повышения качества его работы. Например, в ходе реформ МВД России 2011-2015 годах из органов внутренних дел были уволены 30% сотрудников с одновременным перераспределением их

---

[27] Об организации представления государственных муниципальных услуг: федер. закон от 27.07.2010 г. №201-ФЗ (в ред. от 13.07.2015) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

[28] Путин В.В. Демократия и качество государства [Электронный ресурс]. http://www.kommersant.ru (дата обращения: 22.08.2015)

[29] Касаев И.Х. Совершенствование деятельности органов внутренних дел по предупреждению преступлений, совершаемых участниками этнических преступных группировок // Уголовная политика России на современном этапе: состояние, тенденции и перспективы: сб. науч. ст. Москва: Академия управления МВД России, 2012. С. 198 – 203.

обязанностей на оставшихся сотрудников[30]. В отсутствие качественных изменений технологии работы органов внутренних дел, практика быстро привела руководство страны к осознанию преждевременности данных мер. Поэтому к 2013 году большинство упраздненных подразделений было вновь восстановлено. Сегодня полиция, с одной стороны, постепенно превращается из «органа подавления» в «социальную службу», оказывающую услуги населению. Это подтверждается и законодательно: все последние документы, устанавливающие правила работы органов внутренних дел с гражданами стали называться «Административными регламентами по предоставлению услуг населению». Возрастает значимость вопроса о формах и механизмах взаимодействия полиции и общественности, усиливается роль регулярной отчетности полиции перед обществом. С другой стороны, особое значение приобретает оценка населением деятельности органов внутренних дел – предоставляемой полицией услуги. «Постоянный мониторинг общественного мнения», закрепленный «Дорожной картой дальнейшего реформирования органов внутренних дел Российской Федерации», подразумевает реализацию сплошного наблюдения, когда фиксации подлежат мнения всех граждан.

Но, судя по складывающейся практике, изучение происходит методом случайной выборки – телефонных социологических опросов, что относится к несплошным формам исследований.

В оценке работы сотрудников полиции должны, безусловно, принимать участие не просто граждане, проживающие в районе дислокации отдела полиции, наслышанные о работе правоохранительных органов по сообщениям в прессе и телепередачам, которым позвонили работники социологической службы, выполняющие «опрос населения», а «заявители», то есть лица, имевшие непосредственный контакт с представителями органов внутренних

[30] О внесении изменений в Указ Президента Российской Федерации от 5 мая 2014 г. №300 (О некоторых вопросах Министерства внутренних дел Российской Федерации): Указ Президента Российской Федерации от 13.июля 2015 г. №356 [Электронный ресурс]. http://publication.pravo.gov.ru (дата обращения: 22.08.2015 г.)

дел. Таким образом, информационно- телекоммуникационная модернизация должна осуществляться по двум направлениям.

1. Разработка информационно- телекоммуникационных технологий взаимодействия полиции и общественности, документооборота между ними и отчетности полиции перед обществом. Возможности электронных средств сегодня не используются в деятельности территориальных органов внутренних дел даже наполовину[31]. В работе полиции применяются сети связи, глобальные спутниковые навигационные системы, справочные базы данных[32]. Отдельные госуслуги полиции нашли свое отражение на сайте «Электронного правительства». Но существенно расширить их перечень и внедрить их в полной мере в свою практику пока мешает множество проблем технического характера: отсутствие понятной всем гражданам методики доступа к порталу госуслуг; отсутствие специализированного программного обеспечения для использования этих возможностей в конкретном территориальном органе внутренних дел; отсутствие желания у сотрудников полиции кардинально менять свою работу; и т.д.

Все это приводит к слабому спросу на государственные и муниципальные услуги со стороны населения. Выход из создавшейся ситуации видится нам в повышении доступности гражданам услуг портала «Электронного правительства», расширении его функций за счет перевода всего документооборота между гражданами и полицией в электронную безбумажную форму. Это позволяет сегодня законодательно сделать и Федеральный закон №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» [33] [8], и Приказ МВД России №707 «Об утверждении Инструкции об орга-

---

[31] Семененко Г.М., Герасимов К.Е. Об исторических аспектах развития географических информационных систем в России и зарубежо» // Эволюция современной наук: сб. статей международной научно-практической конференции. Уфа. 2015. С. 182 – 186.

[32] Семененко Г.М. О применение географических информационных систем в деятельности органов внутренних дел по предупреждению преступлений //Сборник научных трудов «Проблемы борьбы с преступностью Российский и международный опыт». Вып. 4. Волгоград. 2014. С. 89 – 94.

[33] О порядке рассмотрения обращений граждан Российской Федерации: федер. закон от 02.05.2006 г. №59-ФЗ (редакции от 24.11.2014) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

низации рассмотрения обращений граждан в си- стеме Министерства внутренних дел Российской Федерации»[34].

Основным инструментом электронного приема обращений от граждан наряду с Интернет- обращениями должны выступать электронные терминалы– аппаратно-программные комплексы, предназначенные для подачи обращений гражданами, предоставления справочной информации, оснащенные сенсорным экраном и специальным программным обеспечением.

Терминалы должны быть установлены в каждом территориальном органе внутренних дел. Они полностью переведут регистрацию обращений граждан в электронный вид и заберут соответствующую функцию у сотрудников дежурных частей, что исключит вероятность уклонений от регистрации информации, отказов гражданам в приеме их сообщений, и других нарушений учетно-регистрационной дисциплины этими сотрудниками. Алгоритм электронного приема обращений от граждан через терминал видится нам следующим образом:

- гражданин, желающий оставить обращение, подходит к электронному терминалу, установленному в отделе полиции,

- сканируют документ подтверждающей их личность (паспорт) в документоприемнике, после чего документ принимается терминалом, на нем отпечатывается время, дата, место приема.

А гражданину автоматически выдается талон-уведомление о принятом обращении. Возможен и другой, безбумажный вариант, когда гражданин заполняет электронный бланк обращения на терминале, в обмен на который также получает талон-уведомление. Сотрудники дежурной части могут устно взаимодействовать с гражданами, при необходимости, оказывать им помощь в подаче обращений. Но они полностью исключаются из процесса регистрации обращений, что существенно снижает количество случаев нарушений служебной дисциплины, повышая качество предоставляемой услуги.

---

[34] Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации: приказ МВД России от 12.09.2013 г. №707 (в ред. от 20.04.2015) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

Использование терминала возможно и в справочно-информационных целях. Посетитель с его помощью может оперативно узнавать все интересующие его сведения о деятельности органа полиции; местах расположения других отелов полиции с указанием их адресов и контактных телефонов; приемных днях руководителей отдела полиции, приемных днях и местах расположения пунктов приема граждан участковыми и их контактных данных; и т.д. Таким образом, электронный терминал будет выполнять отведенные ему функции в составе комплекса инженерно-технических средств информационно-телекоммуникационных технологий, что позволит за счет автоматизации ряда процедур исключить роль человеческого фактора в работе по регистрации обращений; повысить качество фиксации принимаемой информации и уровень ответственности сотрудников полиции при выполнении возложенных на них обязанностей по проверке обращений, принятию решений и информировании о них обратившихся граждан.

Связь электронного терминала с порталом «Электронного правительства» позволит гражданам контролировать работу сотрудников полиции по их обращениям. Для этого гражданам нужно будет пройти облегченную регистрацию на сайте госуслуг и завести там личный кабинет.

Использование представленной нами системы в правоохранительной деятельности будет способствовать:

- получению гражданами в автоматическом режиме в любое удобное время и в удобном месте информации о стадии предоставления услуги полицией;

- автоматическому анализу своевременности выполнения услуг полицией и полноте направленных в адрес гражданина отчетов;

- формированию статистики предоставленных услуг и оценок гражданином качества работы полицейских.

Услуга будет считаться полностью выполненной после принятия полицией решения по обращению и информирования о нем обратившегося гражданина. Кроме того, гражданам, прошедшим регистрацию на портале

госуслуг, будет доступен отчет о работе всех руководителей территориальных подразделений полиции, и возможность оценки работы этих отделов.

2. Разработка информационно телекоммуникационных технологий оценки деятельности полиции населением и сокращения возможностей нарушать права граждан сотрудниками полиции. Инструментом оценки качества работы сотрудников полиции с гражданами может выступать все тот же электронный терминал. Граждане, имевшие опыт общения с сотрудниками полиции, смогут использовать этот электронный терминал еще одним способом – для оценки качества работы сотрудников по оказанию соответствующих услуг. Алгоритм его работы в этом случае видится нам так: гражданин, прибывший в отдел полиции для общения с конкретным сотрудником полиции, должен пройти регистрацию в электронном терминале и указать данные этого сотрудника.

Терминал выдаст гражданину электронную картупропуск, позволяющую пройти к нужному полицейскому. При выходе из отдела гражданин будет обязан вернуть электронную карту в терминал, в ответ на это действие на экране появится таблица, в которой гражданину будет предложено оценить работу полицейского по ряду показателей. Только в этом случае в статистике могут появиться достоверные сведения об оценке деятельности органов внутренних дел гражданами.

Все остальные социологические опросы, безусловно, ценны, поскольку они демонстрируют общее настроение населения в отношении полиции. Но они в себе не несут никакой реальной оценки работы полицейских, поскольку оценивать можно лишь деятельность людей, с которыми непосредственно имел контакт.

В противном случае оценке подвергается только имидж, формируемый средствами массовой информации в сериалах, программах, статьях и т.д.

Таким образом, терминал будет служить многофункциональным устройством, позволяющим гражданам:

- подавать обращения в органы внутренних дел без участия сотрудников полиции и получать документ, подтверждающий их принятие с указанием номера, времени и даты;

- проходить самостоятельную регистрацию для входа на территорию отдела полиции, получать электронный пропуск с возможностью последующей оценки работы полицейского.

По своим функциональным характеристикам предлагаемое оборудование (электронный терминал) и его программное обеспечение не имеет аналогов на современном рынке. Большинство функций, выполнение которых планируется возложить на терминал, сегодня не автоматизировано, производится сотрудниками полиции вручную с помощью бумажных журналов, карточек, пропусков и т.д. Использование электронного терминала самообслуживания в работе органов внутренних дел находится в русле современных тенденций, существенно модернизирует и улучшит качество предоставляемой полицией услуги.

Информационно-телекоммуникационные технологии значительно сокращают сроки получения услуг, позволяют контролировать качество предоставляемой услуги, снижают межведомственную волокиту и количество нарушений служебной дисциплины, повышают комфортность и удовлетворенность граждан от полученной помощи по факту обращения в правоохранительные органы.

Глава 3. Некоторые вопросы использования сотрудниками полиции современных информационных телекоммуникационных систем

3.1. Информационно-коммуникационная система как источник следовой информационной картины о криминальном событии

Информационная служба человечества довольно-таки широка, она охватывает единую систему почтовой, телеграфной, телефонной связи, радиосвязи, книги, газеты и журналы, библиотеки и книгохранилища. Особенно больших успехов достигла в последние годы информационная техника. В настоящий момент с полной уверенностью можно сказать, что двадцать первый век стал веком цифровой техники, электронных средств и коммуникаций, к которым относятся сети сотовой подвижной связи и мобильные радиотелефоны. В настоящее время это одна из самых быстроразвивающихся и перспективных областей электросвязи с массой новых возможностей, операторы которой наступательно реализуют основную цель их создания — обеспечение мобильной связью максимально большего числа абонентов. По данным ведущих операторов сотовой связи, функционирующих на территории РФ (компаний «МТС», «Билайн», «Мегафон»), число их абонентов уже значительно превышает количество пользователей проводных сетей связи.

Однако, чем доступнее становятся средства сотовой связи, тем чаще они используются не просто как инструмент дистанционного человеческого общения, а в качестве средства подготовки и совершения преступлений и для сокрытия следов противоправной деятельности и противодействия расследованию. Анализ следственной практики показывает, что средства связи задействуются при подготовке и совершении заказных убийств, похищения людей, вымогательств, взяточничества, преступлений, связанных с незаконным оборотом наркотических средств, хищений и других общественно опасных деяний. Поэтому становится очевидной необходимость разработки и внедрения адекватных тактических и методических рекомендаций по использованию для

целей расследования информации, обнаруживаемой в средствах сотовых систем подвижной связи.

В этой связи представляется актуальным изучение информационных свойств средств сотовых систем подвижной связи (СССПС) как целостной информационной системы, выступающей в качестве потенциального источника криминалистический значимой информации, а также процесса накопления и формирования сведений об обстоятельствах ее использования конкретным абонентом в качестве источника получения криминалистический значимой информации.

В процессе функционирования мобильной связи принимает участие мобильный телефон, сеть базовых станций и коммутатор. Данный программно-аппаратный комплекс обеспечивает работу: программы, принимающей поступающую от коммутатора информацию, мультиплексора стыкующего коммутатор с ЭВМ, системного программного обеспечения, сетевого оборудования и программного сетевого обеспечения, модема и программного обеспечения модема. При окончании произведенного соединения (в том числе криминального) происходит добавление информации о произошедшем соединении в базу данных этого программно-аппаратного комплекса, управляющего расчетами, т. е. происходит модификация компьютерной информации, механизм образования которой базируется на закономерностях функционирования файловой системы и программ программно-аппаратного комплекса мобильной связи. Следовательно, основными взаимодействующими объектами в процессе установления соединения абонентов посредством средств сотовых систем подвижной связи являются средства информационной поддержки системы мобильной связи (программы, базы данных, данные), а указанный выше аппаратно-программный комплекс представляет собой своеобразный «банк данных» криминалистически значимой компьютерной информации.

Таким образом, принцип организации сети позволяет ее рассматривать как компьютерную, а сам сотовый аппарат в качестве удаленного рабочего

места беспроводной сети. Важно, что сведения о системе мобильной связи как носителе потенциальной криминалистический значимой информации при умелом их использовании могут обеспечивать успех раскрытия и расследования любого преступления.

Характеризуя информацию, обнаруживаемую в СССПС, следует отметить, что она может носить характер как потенциально, так и актуально криминалистический значимой информации. Так, любая информация, возникающая в ходе эксплуатации пользовательского оборудования непосредственно в нем самом и в операционно-информационных системах и центрах коммутации оператора подвижной связи выступает в качестве потенциальной. А характер актуальной она приобретает тогда, когда устанавливается ее прямая причинно-следственная связь с событием преступления (способом преступления, предметами преступного посягательства, лицами, его совершившими, орудиями преступления идр.).

При этом в отличие от обычных криминалистических объектов формой существования этой информации является информационный объект — файл, который обладает фиксированной структурой и определенными параметрами, поддерживаемыми операционной системой.

Ввиду того что сотовая система подвижной связи основана на компьютерной технике (является так называемой интегрированной системой) и обмене компьютерной информацией между ЭВМ коммутатором и периферийным оборудованием — мобильными телефонами, в процессе (установления связи) пользования средствами сотовых систем подвижной связи (как в рамках способа совершения преступления, так и за его пределами) следы контакта редко остаются в виде изменений внешней среды, однако при этом имеют широкое распространение в виде криминалистически значимой компьютерной информации. Они представляют собой всевозможные изменения компьютерной информации — ее уничтожение, модификацию, копирование, блокирование и т. д.

С учетом типовых действий, характерных для пользования абонентом средствами сотовых систем подвижной связи, представляется возможным определить основные типовые следообразующие и следовоспринимающие объекты:

- следообразующий объект — данные и программы аппаратного комплекса, находящиеся в ведении преступника, соучастников;

- следовоспринимающий объект — данные и программы аппаратного комплекса поддержки системы мобильной связи, находящиеся в ведении собственника (оператора мобильной связи).

Представляется необходимым обратить внимание на тот факт, что информация, возникающая в результате использования средств сотовых систем подвижной связи может быть как опосредованной информацией, так и составляющей способа преступления, а соответственно может быть использована для целей раскрытия и расследования преступлений в качестве ориентирующей и доказательственной информации.

Важно иметь ввиду, что информация, обнаруживаемая в СССПС, может быть составляющей способа фактически любого преступления (убийство, разбой, вымогательство и др.), в т. ч. преступлений, совершаемых в сфере мобильных телекоммуникаций (неправомерный доступ к охраняемой законом компьютерной информации; незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного прослушивания и др.). Так, по результатам опроса практических работников было отмечено девять фактов, когда требования или иные условия вымогателей передавались посредством электронной почты или БЫЗ-сообщения.

При этом нельзя не отметить специфичность следовой картины преступлений, совершенных с использованием СССПС по отношению к следовой картине иных преступлений, с одной стороны; и общность ее со следовой картинной ряда преступлений, совершенных с использованием средств компьютерной техники — с другой. Это требует разработки

принципиально иных методов и средств работы с такими следами по сравнению с традиционными.

Результаты анализа практики раскрытия и расследования преступлений с использованием информации, обнаруживаемой в СССПС, свидетельствуют о целесообразности деления информации, возникающей в СССПС и носящей следовый характер, на два вида: следы в традиционном смысле (трасологические) — отображения, вещества, предметы и компьютерно-технические следы.

К первому виду относятся рукописные записи, подписи, выполненные в тексте договора на оказание услуг мобильной связи. Материальные следы могут остаться на корпусе мобильного телефона (следы пальцев рук, микрочастицы). Содержанием компьютерно-технических следов выступает компьютерная информация. При этом компьютерная информация, обнаруживаемая в средствах сотовых систем подвижной связи, являясь подвидом информации в целом, представляет собой сведения, знания или набор команд, предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ, их системе или сети или на машинном носителе, имеющий собственника, установившего правила ее использования.

Компании–операторы сотовой связи фиксируют все голосовые соединения абонента, а также использование им средств мобильного интернета. Аппаратура оператора отражает местонахождение вышки сотовой связи, через которую производится соединение. Это позволяет установить местонахождение абонента с определенной погрешностью на заданный период времени. Фиксируются и уникальные идентификационные номера (IMEI) телефонных аппаратов. Эти данные активно используются правоохранительными органами, ведь такая информация может оказать неоценимую помощь в установлении обстоятельств совершения преступлений и проверки показаний подозреваемых.

Из информации, распространяемой СМИ известно, что детализация телефонных переговоров по множеству уголовных дел служила одним из основных источников доказательств вины.

Рассмотрим способы, которые используются правоохранительными органами для получения и легализации подобных доказательств в уголовном процессе. Сразу необходимо отметить, что информация о телефонных соединениях судебной и иной правоприменительной практикой отнесена к тайне, гарантированной ст.23 Конституции РФ, и доступ к ней возможен только на основании судебного решения.

Итак, существует 3 основных способа получения правоохранительными органами детализации телефонных переговоров:

1. В рамках оперативно-розыскной деятельности. Этот способ регулируется законом «Об оперативно-розыскной деятельности», где в п.11 ст.6 закреплена возможность проведения ОРМ «Снятие информации с технических каналов связи» и осуществляется, как правило, на внепроцессуальных стадиях уголовного судопроизводства. Технически происходят: получение у суда постановления о снятии информации, получение детализации в виде электронных носителей с файлами соединений интересующего абонента, либо эта информация предоставляется на бумажном носителе. В случае возбуждения уголовного дела, по которому полученная информация имеет значение – выносится постановление о предоставлении результатов ОРД в рамках предварительного расследования по уголовному делу.

2. Непосредственно следователем. В 2010 г. законодателем была введена в действие ст.186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Данная норма в определенной степени урегулировала ситуацию по проблеме и регламентировала порядок действий следователя:

а) обращение с ходатайством в суд;

б) направление судебного решения в организацию, осуществляющую услуги связи;

в) проведение осмотра полученной информации по правилам осмотра предметов и документов в присутствии понятых;

г) хранение информации в опечатанном виде.

3. Оперативными работниками. Этот способ — компиляция первого и второго. Следователь дает органу дознания отдельное поручение о проведении ОРМ по снятию информации с технических каналов связи, а орган дознания, выполнив все действия, описанные в пункте 1, передает ее следователю, который проводит осмотр детализации и прочие действия в рамках ст.186.1 УПК РФ.

Анализ сложившейся правоприменительной практики позволяет утверждать, что полученные вышеуказанными способами данные без должной проверки могут не отвечать критерию достоверности.

Разберем техническую составляющую схематично. Каждое соединение абонента фиксируется программным обеспечением оператора сотовой связи. На жестком диске или ином носителе информации, встроенном в оборудование оператора, производится запись в так называемый лог-файл о соединении, вышке сотовой связи, длительности соединения, индивидуальном номере телефонного аппарата. При поступлении постановления суда, разрешающего снятие информации с технических каналов связи, сотрудник оператора копирует лог-файла абонента за необходимый период и распечатывает его.

Выходит, что информацию, имеющую доказательственное значение, правоохранительные органы получают от сотрудника коммерческой организации, который и осуществляет ее копирование, редактирование и т.д. во внепроцессуальном порядке. При этом он не несет никакой ответственности в случае отличия копии от исходной информации. Это делает возможными как случаи предумышленного изменения оригинальных данных в интересах сторон по делу, так и ошибки вследствие технических сбоев или обычной человеческой небрежности.

Случаи расхождения детализации с реальным количеством телефонных соединений нередки. В ходе первого судебного процесса по делу Политковской сын потерпевшей заявил, что количество его звонков матери в день убийства различается с тем количеством, которые отражены в данных оператора связи.

Суд был вынужден сделать повторный запрос оператору, и звонки нашлись, что было объяснено «техническими неполадками».

Одним из важнейших критериев применимости источника информации для его использования в процессе доказывания является критерий достоверности доказательства. В случае, если какая-либо из сторон усомнится в ней, она вправе ходатайствовать перед судом о проведении соответствующих экспертиз. Тем более, если таковые не были проведены на стадии предварительного расследования. Распечатка, переданная оператором связи, проверена быть не может, а вот оригинальный лог-файл – может. На вопросы о дате, времени создания файла, его оригинальности и позднейшем редактировании отвечает судебная компьютерно-техническая экспертиза, самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических.

Учитывая важность использования в рамках уголовного судопроизводства обсуждаемого источника информации, считаю необходимым начать дискуссию о внесении изменений в уголовно-процессуальное законодательство и законодательство, регулирующее деятельность в сфере предоставления услуг связи. Цель — регламентация процесса предоставления данных о соединениях абонента в виде, позволяющем проведение экспертного исследования.

Таким образом, очевидно, что средства сотовых систем подвижной связи представляют собой целостную информационную систему, выступающую в роли потенциального источника КЗИ, которая приобретает характер актуальной по мере выявления ее связи с расследуемым событием. А фрагментарное сходство различных систем связи приводит к необходимости создания более широкого по объему спектра рекомендаций по использованию информации, обнаруживаемой в средствах сотовых систем подвижной связи в деятельности по раскрытию и расследованию преступлений.

3.2. Проблемы производства отдельных следственных действий при расследовании преступлений с использованием информационно-телекоммуникационных систем

В последнее время все большее распространение приобретают преступления, которые совершаются только благодаря возможностям сотовой связи. Так, в настоящее время уже типичными можно назвать действия преступных группприи совершении вымогательства, когда по мобильному телефону предъявляются требования о зачислении на абонентский счет преступника денежных средств за возврат похищенных автомобильных государственных знаков.

Такая же схема используется сотрудниками системы пенитенциарных учреждений при получении незаконного вознаграждения со стороны родственников и знакомых осужденных за совершение действий в их пользу (пронос запрещенных предметов в режимную зону, создание определенных бытовых благ и т. п.).

Настоящей проблемой для органов следствия стали «телефонные» мошенничества, когда по телефону сообщают о необходимости оказания финансовой помощи родственникам, якобы попавшим в сложную жизненную ситуацию (дорожно-транспортное происшествие, болезнь, совершение тяжкого преступления и т. д.).

Сложность расследования такого рода преступлений состоит в отсутствии непосредственного контакта между потерпевшим и преступником, малой материально-следовой базой (как правило, легализация и снятие денежных средств с абонентских счетов (часто неидентифицируемых) происходит мгновенно).

Поэтому информация, полученная в ходе расследования преступления у оператора сотовой связи, является главным, а в некоторых случаях — центральным звеном в цепи доказывания по уголовному делу.

Потребность в получении такой информации у органов предварительного следствия чаще всего возникает после проведения первоначальных следственных действий (осмотра места происшествия, допроса участников процесса, обыска, выемки и др.), когда выясняется, что одним из похищенных предметов стал мобильный телефон, либо, что при совершении преступления злоумышленник использовал средства сотовой связи.

Одной из технических особенностей работы указанных аппаратов в сети оператора сотовой связи (организации связи) является его обязательное подключение к сменному модулю (SIM-карте), позволяющему идентифицировать абонента. Это происходит благодаря техническим возможностям программного обеспечения абонентских устройств, посредством которого данные устройства наделяются индивидуальным 15-значным идентификационным кодом (номером) IMEI, отображающимся в базе данных оператора сотовой связи вместе с номером сменного модуля. Указанный номер относительно постоянен, поэтому информация о нем представляет особую значимость, например, при определении направления передвижения абонента и, соответственно, абонентского устройства. Без модуля телефонный аппарат может функционировать только в ограниченном режиме — для соединений с экстренными службами.

Следователю необходимо учитывать, что в одном и том же телефонном аппарате могут использоваться как одновременно, так и разновременно несколько SIM-карт. Они могут меняться, переставляться в другие телефоны и гаджеты, данные номеров нередко вводятся абонентами при пользовании интернет-ресурсами.

В связи с тем, что оператор сотовой связи получает в централизованные базы данных информацию обо всех произведенных абонентом манипуляциях с аппаратом, с использованием модуля SIM, после хищения преступники пытаются извлечь данный модуль, перепродать либо уничтожить его за ненадобностью. Как правило, похищенные сменные модули используют лица, которые не осведомлены об особенностях работы мобильных средств связи в

сети. Такими лицами чаще всего являются несовершеннолетние, использующие телефон в целях получения доступа к сети Интернет, а также лица, которые впервые совершили преступление.

Подготовка к получению информации о соединениях между абонентами и (или) абонентскими устройствами складывается из последовательно сменяющих друг друга этапов:

- подбор и изучение материалов уголовного дела, анализ сведений об абоненте и (или) об абонентском устройстве, а также о лице, чья абонентская активность будет проверяться;

- определение цели и конкретных задач данного следственного действия;

- вынесение постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами;

- получение согласия руководителя следственного органа на проведение данного следственного действия;

- получение судебного решения;

- направление копии постановления суда в организацию связи.

Рассмотрим названные этапы более подробно.

Анализ ситуации и сбор данных. Перед тем как принять решение о необходимости получения информации у операторов сотовой связи, следователь должен удостовериться в том, что представленные сведения могут иметь значение для уголовного дела. Например, подтверждением того, что мобильный телефон был похищен у потерпевшего в результате грабежа, может служить представленная им товарно-кассовая документация на телефон, выемка оставшихся у потерпевшего аксессуаров, показания свидетелей происшедшего, потерпевшего и др.

В случае если информация о хищении абонентского устройства или использовании мобильного телефона в ходе преступления подозреваемым подтверждается, следователь определяет идентификационные признаки

абонентского устройства, приблизительное место его последнего использования.

Для этого проводится допрос потерпевшего, в ходе которого выясняется: дата, время, место приобретения абонентского устройства, серийный номер, наличие документов, абонентский номер и организация сотовой связи, где оформлен договор о предоставлении услуг, стоимость телефона (наличие кассового чека); описание абонентского устройства: цвет корпуса (отдельных панелей), наличие чехла и иных аксессуаров, отличительные признаки, механические повреждения либо метки, особенности работы. Особое внимание следует уделять информационному содержимому встроенных и/или съемных носителей информации: контактов, фото-, видео- и аудиофайлов, так как именно эти сведения запечатлеваются в памяти потерпевшего и могут в дальнейшем помочь, в том числе при опознании средства сотовой связи.

Очень важно после проведения допроса и получения идентификационных данных абонентского устройства (номер IMEI, SIM) направить запросы в организации связи, работающие в месте производства предварительного расследования с тем, чтобы установить, пользуются ли их услугами связи интересующие следствие лица (ч. 4 ст. 21 УПК РФ). На данном этапе при ответе на такие запросы организации связи ограничиваются формулировками о наличии или отсутствии регистрации запрашиваемого абонента и (или) абонентского устройства в сети. Поэтому направление запроса операторам сотовой связи не требует получения судебного решения.

Определение круга вопросов к оператору. После получения от организации связи положительного ответа о факте регистрации абонента и (или) абонентского устройства следователь определяет круг вопросов, на которые может ответить организация связи. К ним может относится информация:

- о номере модуля SIM, используемого в интересующем средстве сотовой связи, и, соответственно, сведения о ее владельце (абоненте);

- о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи (так называемая детализация);

- о координатах места осуществления соединений с помощью интересующего следствие абонентского устройства;

- о координатах местонахождения абонента и абонентского устройства при подключении его к сети (так называемая геолокация).

Возбуждение ходатайства перед судом. Правовым основанием получения информации о соединениях между абонентами и (или) абонентскими устройствами является судебное решение, вынесенное по ходатайству следователя с согласия руководителя следственного органа.

Уголовно-процессуальный закон устанавливает, что в ходатайстве о производстве следственного действия указываются: номер уголовного дела; основания, по которым производят следственное действие; период, за который необходимо получить соответствующую информацию, и (или) срок производства следственного действия; наименование организации, от которой необходимо получить указанную информацию (ч. 2 ст. 186.1 УПК РФ).

В ходатайстве о получении информации о соединениях между абонентами и (или) абонентскими устройствами и соответствующем судебном решении также следует указать, кому необходимо передать (направить) сведения о соединениях между абонентами и (или) абонентскими устройствами (указать на необходимость передачи информации конкретному сотруднику или направить ее почтой с указанием почтового адреса).

При этом вне зависимости от места расположения следственного отдела ходатайство о проведении следственного действия должно подаваться в суд, юрисдикция которого распространяется на территорию, где было совершено преступление, либо, где проводится следственное действие.

Так, в рамках расследования уголовного дела следователь с согласия руководителя следственного органа обратился в Бабушкинский районный суд г. Москвы с ходатайством о разрешении получения сведений об абонентской активности.

Суд в рассмотрении этого ходатайства отказал по тем снованиям, что предположительное место совершения преступления, а также место следственного действия расположены на территории, которая не относятся к юрисдикции Бабушкинского районного суда г. Москвы, в связи с чем рассмотрение ходатайства следователя не подсудно данному суду.

В кассационном представлении прокурор выразил свое несогласие с постановлением суда, мотивируя это тем, что следственное подразделение расположено по адресу, который относится к территории Бабушкинского районного суда. Рассмотрев данное представление, судебная коллегия по уголовным делам Московского городского суда признала доводы прокурора несостоятельными и не подлежащими удовлетворению[35].

В данном случае судебная коллегия воспользовалась правилом аналогии, обосновывая свое решение позицией Конституционного Суда РФ, выраженной ранее в постановлении от 20.07.2012 № 20-П[36].

Напомним, что данным постановлением устанавливается безотносительность места расположения межрайонных следственных органов к юрисдикции судов муниципальных образований в случаях обжалования решений и действий (бездействия) следователей.

Немаловажно отметить, что перед обращением в суд с ходатайством о получении информации о соединениях абонента сотовой связи следователь должен постараться смоделировать поведение потерпевшего и преступника, определить для себя уровень информационно-технологической грамотности преступника. При этом попытаться расширить возможности следствия в получении необходимой информации от оператора.

Следует обратить внимание на то, что наряду с ходатайством о получении абонентской информации следователь должен представить в суд заверенные гербовой печатью копии постановлений о возбуждении уголовного дела,

---

[35] Кассационное определение от 24.10.2012 по делу № 22-14391/2012// СПС ГАРАНТ

[36] Постановление КС РФ от 20.07.2012 № 20-П «По делу о проверке конституционности положений части первой статьи 125 и части первой статьи 152 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой гражданки Р. Г. Мишиной» // Российская газета. 2012. 08 авг.

принятия уголовного дела к производству, продлении либо возобновлении срока предварительного расследования, а также заверенные копии материалов, подтверждающих законность и обоснованность данного решения (протоколы осмотров, допросов, обысков и т. д.). Техническому исполнителю следственного действия (оператору сотовой связи) в обязательном порядке также направляется заверенная копия постановления суда.

Взаимодействие с оператором и получение информации. Организация связи обязана передавать следователю указанную в судебном решении информацию по мере ее поступления не реже одного раза в неделю (ч. 4 ст. 186.1 УПК РФ). Тем не менее, по устоявшейся практике, информация представляется инициатору оператором сотовой связи только после того, как контролируемый абонент и (или) абонентское устройство регистрируются в сети, либо в срок, который следователь отдельно указывает в ходатайстве (например, в течение 12 часов с момента регистрации в сети).

Взаимодействие следователя и оператора сотовой связи может осуществляться длительный период времени, но не более 6 месяцев. В случае если для уголовного дела имеет значение информация о соединениях, которые предшествовали принятию судебного решения, она может истребоваться следователем за неограниченный период.

Если необходимость в производстве данного следственного действия отпадает, оно прекращается по постановлению следователя, но не позднее окончания предварительного расследования по уголовному делу (ч. 7 ст. 186.1 УПК РФ).

В этой связи А. Н. Гуевым указывается на противоречие положений ст.ст. 13, 29, 164, 165 и ст. 186.1 УПК РФ, выражающееся в том, что судебное решение, которым было разрешено проведение данного процессуального действия, отменяется не в судебном порядке, а по решению следователя. Как справедливо утверждает автор, «законодателю целесообразно еще раз

вернуться к данному вопросу и сделать прекращение следственного действия прерогативой суда»[37]

Интересующая следствие информация должна быть представлена руководителем организации связи в опечатанном виде с сопроводительным письмом, где указываются период, за который она предоставлена, номера абонентов и (или) абонентских устройств. Сведения могут быть переданы на любом носителе информации. Чаще всего для этого используются офисная бумага или стандартные CD-диски, либо съемные накопительные устройства (флэш-карты).

Полученные следователем документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, подлежат обязательному осмотру. Если осуществляющая услуги связи организация представила информацию в электронном виде (на электронном носителе или диске), следователь обрабатывает ее с помощью компьютера, что поэтапно фиксируется в протоколе осмотра. Для обработки кодированной информации или представляющей большой объем к осмотру следует привлекать специалистов в области программного обеспечения сетей сотовой связи.

В протоколе осмотра документа, содержащего информацию о соединениях между абонентами и (или) абонентскими устройствами, указываются: наименование организации, представившей информацию; состояние и обозначения упаковки; материал, из которого изготовлен носитель; размеры, цвет, внешний вид, идентификационные сведения; дата и время соединений; признак исходящего или входящего вызова абонента; номер абонента (кому или кто звонил) или уникальный код идентификации; продолжительность соединения в секундах и другие данные (ч. 5 ст. 186.1 УПК РФ). К последним, очевидно, могут быть отнесены паспортные данные абонента, сведения из базы данных систем расчета за оказанные услуги связи, в

[37] Гуев А. Н. Постатейный комментарий к Уголовно-процессуальному кодексу Российской Федерации [Электронный ресурс], Доступ из СПС «Гарант», 2016.

том числе и платежах абонента, информация о номерах и месте расположения приемопередающих базовых станций и др.

При этом если осматриваются документы на электронном носителе, следует указывать все манипуляции с компьютерным оборудованием и программным обеспечением, необходимые для доступа к информации. В некоторых случаях по усмотрению следователя при особой важности получаемой информации может быть применена фото- и видеосъемка.

Получив данные о сотовых соединениях абонентов (как правило, они громоздки), следователь должен не просто осмотреть их, но и подробно проанализировать принадлежность номеров, время контактов, очертить круг контактов потерпевшего, а возможно, и преступника. К сожалению, на практике осмотр часто нивелируется указанием неполной информации о том или ином контакте или абоненте.

Лица, участвующие в осмотре и анализе представленных документов, вправе в том же протоколе или отдельно изложить свои замечания к протоколу. Такой порядок осмотра необходим, прежде всего, для того, чтобы не была упущена вышеуказанная информация.

Согласно ч. 6 ст. 186.1 УПК РФ документы, содержащие информацию о соединениях между абонентами, приобщаются к материалам уголовного дела в полном объеме в качестве вещественных доказательств, о чем выносится соответствующее постановление, и хранятся в опечатанном виде.

Главным отличием протокола следственного действия, составленного по результатам осмотра представленных документов, является то, что первичная информация извлекается субъектом доказывания не из следов, оставленных преступником, а путем оставления следа опосредованным, по сути, комбинированным объектом. Таким объектом, как правило, выступает носимое средство сотовой связи с активированным в нем сменным абонентским модулем (SIM), которое и является при формировании доказательства «носителем искомой информации» о событии, произошедшем в определенном месте и в определенное время.

По мнению А. Ю. Шапошникова, чтобы использовать в доказывании информацию об абонентах, полученную у операторов сотовой связи, необходимо установить и доказать множество промежуточных фактов. Например, что в тот или иной момент устройство находилось в руках конкретного лица, что именно это лицо использовало конкретный абонентский номер и т. п. Для этого, как отмечает ученый, потребуется доказывать отсутствие номеров и устройств-двойников, изучать возможную подделку SIM-карт и изменений уникальных номеров сотовых устройств (IMEI)[38].

Таким образом, можно констатировать, что информация, полученная в рамках следственного действия, регламентированного ст. 186.1 УПК РФ, имеет только косвенное доказательственное значение. Но, как всякое косвенное доказательство, сведения об абонентах (пользователях), состоящие в гармоничной системе с другими доказательствами, могут вырасти «в страшную, неотвратимую силу, превращаются в цепь доказательств, окружающих обвиняемого глухой стеной, через которую нельзя прорваться, нельзя никуда уйти».

Об этом свидетельствует и судебно-следственная практика.

08.10.2008 в г. Астрахани был обнаружен труп гражданки Х.

Судебно-медицинская экспертиза установила, что смерть наступила от механической асфиксии в результате сдавливания шеи. В ходе следствия удалось выяснить, что в квартиру под видом клиентов-квартиросъемщиков проникли двое иногородних мужчин. Убив женщину и не обнаружив в доме денег, преступники забрали только сотовые телефоны.

Следователь, расследовавший это уголовное дело, направил запрос в компанию сотовой связи, откуда поступила информация, которая позволила установить одного из участников убийства. Комплекс последующих мер

[38] Шапошников А. Ю. Ходатайство о получении информации об абонентах должно быть обоснованным // Уголовный процесс. 2016. № 10. С. 43.

позволил установить и задержать по «горячим следам» и второго преступника[39].

Федеральным законом от 01.07.2010 № 143- ФЗ7[40] законодатель попытался, и не совсем безуспешно, «разрубить гордиев узел». Напомним, что диспуты о форме, порядке истребования сведений, необходимости получения судебного решения, как на страницах научной литературы, так и служебных кабинетах, до принятия закона разгорались каждый раз с новой силой.

Между тем новелла также не дает ответа на ряд вопросов, которые возникают в процессе применения норм указанной статьи.

Возможность получения информации о содержании электронных сообщений. Так, в настоящее время в качестве доказательств по уголовному делу следственными органами широко используются сведения об отправке, принятии и содержании электронных сообщений (SMS, EMS, MMS, ISQ и др.) в случае, когда они передавались в момент подготовки и (или) совершения преступления.

По приговору Верховного суда Республики Марий Эл от 27.08.2007 Т. был осужден по п. «з» ч. 2 ст. 105 УК РФ. В ходе судебного заседания осужденный и его адвокат утверждали, что Т. не причастен к убийству Ч. и что приговор постановлен на недопустимых доказательствах: заявлении о явке с повинной и первоначальных показаниях, где он признавал свою вину, от которых впоследствии отказался.

Судебная коллегия по уголовным делам Верховного Суда РФ оставила без изменения приговор Верховного суда Республики Марий Эл, а кассационные жалобы — без удовлетворения, указав, что суд, исследовав представленные стороной обвинения доказательства, одним из которых являлась приобщенная к уголовному делу распечатка SMS-сообщений, обоснованно признал Т. виновным в убийстве Ч.[41].

---

[39] Предполагаемых убийц астраханки выдал сотовый телефон // ИА REGNUM [Электронный ресурс]. URL: www.regnum.ru (дата обращения: 06.06.20137).

[40] Российская газета. 2010. 07 июля.

[41] Определение от 12.11.2007 № 12-О-07-22// СПС ГАРАНТ

В то же время остается открытым вопрос о возможности получения сведений о содержании электронных сообщений по процедуре, предусмотренной ст. 186.1 УПК РФ. Например, по мнению Н. А. Архиповой, это вполне допустимо[42].

Основываясь на определении термина, указанном в п. 24 ст. 2 Федерального закона от 07.07.2003 № 126- ФЗ «О связи», можно считать, что «сеть сотовой связи» — это технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи.

В пункте 2 постановления Правительства РФ от 23.01.2006 № 32 «Об утверждении Правил оказания услуг связи по передаче данных»[43] говорится, что «соединение по сети передачи данных (сеанс связи) — установленное в результате вызова или предварительно установленное взаимодействие между средствами связи, позволяющее абоненту и (или) пользователю передавать и (или) принимать голосовую и (или) неголосовую информацию».

Используя эту формулировку, представляется целесообразным под соединением между абонентами (или) абонентскими устройствами понимать установленное в результате вызова или предварительно установленное взаимодействием между абонентскими устройствами, позволяющее абоненту и (или) пользователю передавать и (или) принимать неголосовую информацию.

Пункт 24.1 ст. 5 УПК также содержит формулировку: «…других данных, позволяющих идентифицировать абонентов…», которая предполагает включение в контекст запрашиваемых у оператора сотовой связи сведений о соединениях, осуществляемых посредством принятия или отправки электронных сообщений. Между тем информационное содержание сообщений, представляющее собой набор символов, набираемых пользователем устройства связи, идентифицируется оператором только после их отправления/принятия.

Резюмируя сказанное, можно сделать вывод, что получение сведений об информационном (знаковом, графическом) содержании электронных

[42] Архипова Н. А. Об использовании SMS-сообщений в ходе раскрытия и расследования преступлений // Вестник Санкт-Петербургского университета МВД России. 2015. № 4 (48). С. 55.
[43] Российская газета. 2006. 10 июля.

сообщений в рамках проведения следственного действия, регламентированного ст. 186.1 УПК РФ, является неправомерным.

Получение информации о неустановленном круге абонентов. До конца не разрешенным остается и вопрос о возможности получения информации о неустановленном круге абонентов, которые находились в определенном месте и в определенный промежуток времени. Как показало изучение судебной практики, в этом случае судом неоднозначно применяются нормы ст. 186.1 УПК РФ.

Так, дознаватель обратился в суд с ходатайством, согласованным с первым заместителем прокурора г. Москвы, о разрешении получения у оператора сотовой связи информации о входящих и исходящих соединениях всех абонентских номеров, относящихся к «номерной емкости» оператора, находившихся в непосредственной близости к месту происшествия, с указанием IMEI номеров аппаратов, базовых станций, через которые происходило соединение, вектора направления на них, с предоставлением сведений о лицах, на которых зарегистрированы абонентские номера.

Постановлением Тверского районного суда г. Москвы от 11.09.2012 в удовлетворении данного ходатайства было отказано.

В кассационном представлении прокурор выразил несогласие с постановлением суда, считая его незаконным, необоснованным и подлежащим отмене.

Ссылаясь на установленные дознанием фактические обстоятельства дела, прокурор утверждал, что дознаватель обратился в суд с ходатайством в полном соответствии с требованиями ст.ст. 29, 165, 23.1, 186.1 УПК РФ, в связи с необходимостью проведения следственного действия, а не оперативно-розыскного мероприятия.

По мнению прокурора, выводы суда, изложенные в постановлении, противоречат ч. 2 ст. 186.1 УК РФ, а получение информации о соединениях между неопределенным кругом абонентов и (или) абонентских устройств не

может повлечь нарушение прав граждан, установленных в ст. 23 Конституции РФ и ст. 13 УПК РФ.

Судебная коллегия по уголовным делам Московского городского суда 31.10.2012 нашла постановление суда законным и обоснованным. По мнению судей, исходя из содержания нормы ч. 1 ст. 186.1 УПК РФ, получение информации, о которой указывает дознаватель, может привести к необоснованному ограничению прав неопределенного числа граждан на тайну телефонных переговоров, что противоречит требованиям ст. 23 Конституции РФ и ст. 13 УПК РФ.

Таким образом, постановление Тверского районного суда г. Москвы от 11.09.2012 судебной коллегией было оставлено без изменения, а кассационное представление прокурора — без удовлетворения[44].

Между тем 20.03.2013 тот же судебный орган выносит апелляционное определение по уголовному делу, возбужденному по ч. 1 ст. 105 УК РФ. Данным определением он отменяет постановление суда об отказе в удовлетворении ходатайства следователя о производстве следственного действия, предусмотренного ст. 186.1 УПК РФ.

Судебная коллегия сочла несостоятельными выводы суда первой инстанции о незаконности получения абонентской информации неопределенного круга лиц в связи с тем, что возможно несанкционированное получение сведений о телефонных соединениях лиц, в отношении которых применяется особый порядок производства по уголовным делам.

В итоге, отменяя в связи с изложенным постановление суда, судебная коллегия пришла к выводу, что ходатайство следователя отвечает требованиям ч. 2 ст. 186.1 УПК РФ и подлежит удовлетворению, поскольку из материалов дела следует, что запрашиваемая информация имеет значение для уголовного дела и установления лица, совершившего 12.02.2013 особо тяжкое преступление, по факту которого было возбуждено дело[45].

---

[44] Кассационное определение от 31.10.2012 по делу № 22-14801/12// СПС ГАРАНТ

[45] Апелляционное определение Московского городского суда от 20.03.2013 по делу № 10-907// СПС ГАРАНТ

Представляется, что в двух приведенных судебных решениях наиболее верной является позиция органов предварительного следствия. Во-первых, она основывается на нормах ч. 2 ст. 186.1 УПК РФ, которыми не предусматривается конкретизация данных абонента или абонентских устройств; во-вторых, фактическим основанием производства данного следственного действия является небезосновательное предположение дознавателя (следователя) о том, что подозреваемый на момент совершения преступления может являться абонентом сотовой связи и одновременно пользователем мобильного телефона, который в процессе совершения преступления находился в его одежде, сумке или другой ручной клади.

При этом не исключено, что подозреваемый на месте совершения преступления или в непосредственной близости от него мог использовать мобильный телефон: осуществлять звонки, получать или отправлять сообщения, проверять баланс, совершать иные манипуляции, которые были отражены в информационной среде баз данных оператора сотовой связи. Тем более что следственная практика пестрит примерами, когда правоохранительным органам удавалось раскрыть преступление «по горячим следам» благодаря именно такому поведению преступников на месте преступления и полученным об этом сведениям у операторов сотовой связи.

Так, в прокуратуру поступило заявление от М. о безвестном исчезновении его дочерей. В ходе расследования установлено, что М. осуществлял совместно с дочерьми торговлю промышленными товарами и одеждой на рынке. Окончив торговлю, они выехали по направлению домой. В машине находились деньги в сумме 58 тыс. руб. и товар на сумму 400 тыс. руб. На автозаправочной станции между М. и дочерьми произошел конфликт, после чего тот ушел. Спустя час он вернулся, однако автомашины и дочерей не обнаружил.

На следующий день в ходе организованных поисков в лесопосадке в 3 км от близлежащего населенного пункта были обнаружены трупы сестер М. с огнестрельными ранениями головы. Незамедлительно принятыми мерами были

получены протоколы соединений, произведенных с похищенного мобильного телефона одной из потерпевших. При проверке выявлен телефонный номер абонента К., на который произведен звонок непосредственно перед выключением телефона.

На установленный адрес была направлена следственно-оперативная группа. При проведении обыска домовладения К. и осмотре прилегающей территории обнаружена автомашина М. с частично демонтированными деталями и следами крови в салоне, а также имущество, принадлежащее потерпевшим. По подозрению в совершении преступления задержан К. и его сын К.А., которым впоследствии было предъявлено обвинение в совершении преступлений, предусмотренных п.п. «а», «з» ч. 2 ст. 105, п. «а» ч. 4 ст. 162 УК РФ[46].

Считаем неверной позицию судов, которые подходят избирательно к ходатайствам следователя о получении абонентской информации, разделяя все преступления на две группы: представляющие и не представляющие повышенную общественную опасность. К первой группе судьи, как правило, относят преступления небольшой и средней тяжести, ко второй — тяжкие, особо тяжкие преступления или отдельные виды преступлений (террористической направленности и т. п.).

Калманским районным судом Алтайского края было отказано в удовлетворении ходатайства о выемке информации у ряда операторов сотовой связи о всех соединениях, осуществленных через базовые станции операторов, в зоне действия базовой станции, обслуживающей территорию в районе места совершения преступления.

Суд руководствовался тем, что тяжесть совершенного преступления и его обстоятельства не являются основанием для нарушения конституционных прав

[46] Об организации расследования преступлений, связанных с хищением средств сотовой связи: Методические рекомендации. Волгоград, 2015. С. 5.

на тайну телефонных переговоров большого числа лиц, не причастных к совершению преступления[47].

В соответствии с ч. 2 ст. 21 УПК РФ обязанность следователя (дознавателя) в каждом случае обнаружения признаков преступления принимать предусмотренные УПК меры по установлению события преступления, изобличению лица (лиц), виновных в его совершении. В целях обеспечения полного и всестороннего расследования следователь (дознаватель) должен применить весь арсенал законных средств и методов, используя, в том числе, технические возможности организаций связи. Поэтому при разрешении ходатайства о проведении следственного действия суд должен исходить из позиции приоритетности преступлений, представляющих повышенную общественную опасность, но не из их исключительности.

В этой связи представляется обоснованной позиция КС РФ, нашедшая отражение в определении от 02.10.2003 № 345-О[48]: «… судья обязан не допускать сужения сферы судебного контроля, субъективно оценивая фактические данные, влекущие необходимость получения судебного решения, ограничивающего права на тайну телефонных переговоров, которое имеет целью обеспечение интересов общества и государства, составляющих в единстве с интересами личности совокупность национальных интересов России. Этим обусловливается обязанность судьи, рассматривающего ходатайство органов, осуществляющих оперативно-розыскную деятельность, о производстве действий, связанных с ограничением права на тайну телефонных переговоров, подходить к оценке представляемых в таких случаях материалов ответственно и всесторонне».

Эффективная борьба с преступностью зависит от уровня организации следственной, оперативной, профилактической работы, проводимой сотрудниками органов министерства внутренних дел (ОМВД). Результат такой

---

[47] Об организации расследования преступлений, связанных с хищением средств сотовой связи: Методические рекомендации. Волгоград, 2015. С. 5.

[48] Определение КС РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда г. Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи» // Вестник Конституционного Суда РФ. 2004. № 1. С. 52.

работы будет зависеть от качества информационной поддержки, так как основные усилия сотрудников органов внутренних дел (ОВД) в предотвращении, раскрытии и расследовании преступлений связаны с получением информации. Именно данные функции и должна обеспечивать система информационного обеспечения ОВД. Постоянно расширяется и круг потребителей, которые заинтересованы в получении необходимой информации, имеющейся в подразделениях ОВД. Если ещё несколько лет назад данную информацию использовали, в основном, оперативно-следственные работники ОМВД, прокуратуры, службы безопасности, то в наше время её используют сотрудники таможенной и налоговой служб, коммерческих и финансовых структур, представители республик, администраций, краев, областей. Работы, связанные с автоматизацией информационного обеспечения ОВД ведутся с начала 70-х г. Первые информационные центры оснащались компьютерами типа «Минск-22», «Минск-32», затем ЭВМ типа «ЕС» и «СМ», которые использовались для обработки статистических данных. Отсутствие развитых программных средств и слабость технических баз данных и не позволяли осуществлять концепцию единой базы данных[49]. Сейчас большинство региональных ОМВД России используют современные информационные системы в своей деятельности. Используемые системы могут иметь собственный язык управления данными, свои форматы и потоки данных, свои решения в части выбора технических средств и архитектуры. Использование такого подхода может сделать невозможным в будущем реализацию единого информационного пространства. Очевидна необходимость в разработке и использовании единой информационной системы обслуживания массового пользователя[50].

[49] Ваулина Т.Н. Преступления в сфере компьютерной информации // Уголовное право / отв. ред. И.Я. Козаченко и др. – М.: ИНФРА-М-НОРМА, 2016. – С. 559.

[50] Михед А.Д., Безгубова А.А. Использование правоохранительными органами интернета и телекоммуникационных систем для получения информации о криминальном событии. / Известия ТулГУ. Экономические и юридические науки. Вып. 3. Ч. II. – Тула: Изд-во ТулГУ, 2015. - С. 146-150.

Такой единой информационной системой может являться программная среда UTSPolice[51], которая предназначена для информирования граждан о деятельности ОМВД; обработки электронных обращений (сообщений) граждан и предоставление информации об услугах (контакты, обратная связь, справка, добровольная дактилоскопическая экспертиза и т.п.); отображений фотографий лиц, находящихся в розыске и т.д. В системе UTSPolice обратная связь реализована следующим образом: любой гость, через Интернет, может записаться на прием к руководителям ОМВД (выбрав сотрудника, время, свободную дату посещения и получив возможность записаться на прием, система запрашивает контактный телефон для обратной связи). Мониторинг мнения общественности происходит с помощью онлайн опросов, таких как «Ваше мнение о работе полиции» «Рейтинг лучшего участкового полиции» и т.д. Контактные данные в отношении руководства ОМВД в системе UTSPolice демонстрируются с отправкой письма на электронный почтовый ящик с номерами телефонов сотрудников полиции. При этом необходимо отметить, что все электронные ящики руководителей настроены на СМС- оповещения о получении письма. UTSPolice, так же, позволяет пользователю наглядно посмотреть карту города, с разметками и обозначениями зон обслуживания участковых уполномоченных полиции. При просмотре информации об участковых полиции высвечивается карта, которая разделена на административные участки города. При выборе на экране цифры, обозначающей административный участок, гражданин может посмотреть контакты участкового, закрепленного на данной территории, и написать ему письмо. Оказание услуг с помощью сети Интернет позволяет посетителю сохранять нужную информацию на запоминающее устройство (USB-носитель).

Так например, любой человек может сохранить необходимые образцы заявлений, бланки, различные документы и т.д. Столь же доступны стали услуги лицензионно-разрешительного отдела ОМВД и получения информации

[51] Использование программно-аппаратного комплекса для оказания электронных услуг населению [Электронный ресурс]. – Режим доступа: http://www.ormvd.ru/pubs/102/15612/ (Дата обращения: 18.06.2017).

о розыске опасных преступников: бегущая строка присутствует на каждой web-странице и имеет функции перехода на вкладку «Розыск». Переход на web-сайты государственных структур РФ и административного региона происходит с использованием программы UTSBrowser.

Таким образом, система UTSPolice представляет собой программно-аппаратный комплекс, который состоит из персонального компьютера, с доступом в Интернет, специализированного программного обеспечения и сенсорного монитора. На основании официального запроса сотрудники полиции могут получать в своё распоряжение самые различные данные, начиная с занятий какой-либо деятельности физического или юридического лица и кончая использований средств сотовой связи, а так же социальных сетей. Запрашивать нужную информацию в связи с находящимися в производстве делами об административных правонарушениях, расследуемыми уголовными делами, а так же в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях являться правом ОВД.

Диапазон правонарушений, которые выявляются с использованием Интернета, достаточно велик. Преступник, находящийся в розыске, может пользоваться социальными сетями («Одноклассники», «Facebook», «Vkontakte» и др.) и обсуждать там ограбление банка или заказное убийство. В этом случае сотруднику полиции для определения информации о преступники (номер сотового телефона, IP-адрес компьютера, переписка) необходимо направить официальный запрос в техническую поддержку социальной сети, предварительно написав им сообщение в сети Интернет. Запрос в ООО «В контакте» может быть направлен по адресу – 191040, г. Санкт-петербург, Лиговский проезд, д. 61, литер А.; а запрос в ООО «Одноклассники» - 125167, г. Москва, Ленинградский проспект, д. 39, строение 79, БЦ «SkyLight» на имя генерального директора управляющей организации ООО «Интернет компания

Мэйл.Ру» Багудиной Е.Г[52]. Противодействия преступлениям в сфере информационных технологий оказывает бюро специальных технических мероприятий (БСТМ) МВД, которое получило название – отдел «К». В процессе своей работы сотрудники полиции при возбужденном уголовном деле, а так же в рамках материалов проверки, обращаются с запросом к отделу «К» для получения необходимой информации, в рамках решаемых задач[53].

Предположим, что сотруднику полиции необходимо узнать телефон злоумышленника, который пользуется оператором Теле2 и зарегистрирован в социальной сети, тогда официальный запрос от сотрудника может быть направлен как в БСТМ, так и в техническую поддержку сайта или офис компании Теле2. В свою очередь БСТМ непосредственно взаимодействует с компаниями сотовых операторов, от которых и получает необходимую информацию. На рисунке показана структурная схема запросов на определение номера сотового телефона злоумышленника от ОМВД.

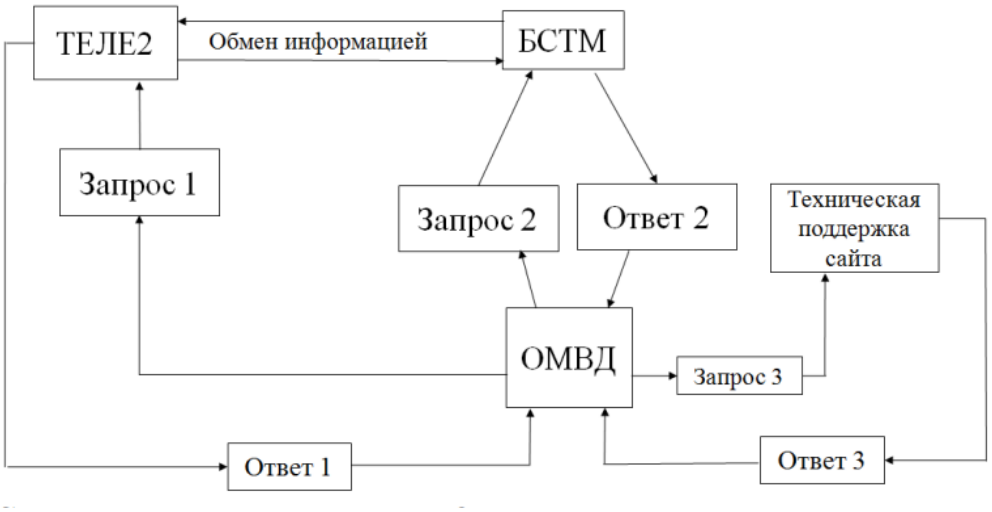

Рис. Структурная схема запросов ОМВД на определение номера сотового телефона

[52] Полиция в социальной сети. Newsland. [Электронный ресурс]. – Режим доступа: http://newsland.com/ (Дата обращения: 18.06.20157).
[53] Управление «К» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Управление_К (Дата обращения: 18.06.2017).

Отправка запроса в техническую поддержку социальной сети может быть полезна в том случае, если преступник использует сим-карту, оформленную на чужое имя, но в тоже время при регистрации в социальной сети указал на сайте номер сотового телефона данной сим-карты. При этом запросы в БСТМ и Теле2 ожидаемых результатов (ответов) не принесут, т.к. в базах данных сотовых операторов преступник числится не будет. Не менее важным является время ожидания ответа с момента отправки запроса сотрудником полиции. Так как запрос в техническую поддержку отправляется по почте (в бумажном варианте), то время ожидания ответа будет зависеть от дальности между регионом ОМВД и центральным офисом социальной сети, и может составить более месяца. Ответ из БСТМ готовится около месяца, а ответ из центрального офиса сотовой связи в течении 10 рабочих дней.

Таким образом, использование информационных систем и социальных сетей для получении информации о преступнике, в силу стремительного развития информационных технологий, становится все более актуальным и требует дальнейшего развития и изучения. Система UTSPolice значительно упрощает взаимосвязь между гражданином и территориальным органом. Кроме того, использование подобных систем службами собственной безопасности ОМВД органов может помочь в выявлении нарушений среди личного состава служащих.

ЗАКЛЮЧЕНИЕ

Представим основные выводы по работе.

1. Современные информационные процессы представляют собой одну из наиболее важных составляющих социальной, экономической и политической деятельности человека и общества. Ключевую роль в развитии современного общества играют информационные технологии, без использования которых стала немыслимой деятельность и функционирование важнейших институтов человеческой цивилизации.

2. ИКТ сегодня активно используются правоохранительными органами в их профессиональной деятельности. Ведомственная ИСОД, например, активно применяется для проведения служебных совещаний. Она содержит множество информационных сегментов, открывающих доступ к обширной базе самых разнообразных сведений, в том числе к оперативным, справочным и криминалистическим централизованным учетам. Распространена также практика оборудования отдельных подразделений локальными компьютерными сетями, что облегчает циркуляцию служебной информации внутри них.

Повсеместно сегодня применяются электронная почта, IP-телефония и факсимильная связь. Необходимо отметить, что далеко не все приведенные способы использования ИКТ можно охарактеризовать как технико-криминалистические, поскольку информация, поступающая посредством таких каналов, относится к категории ориентирующей. На сегодняшний день ИКТ для обнаружения и фиксации доказательств не применяются.

3. На сегодняшний день методика использования информационных технологий при расследовании преступлений должна базироваться на следующих компонентах:

– сегментирование отдельных следственных действий (их этапов – подготовка, проведение, фиксация хода и результатов) на базе повсеместного использования информационных технологий на каждом из таких этапов.

– осуществление программного сопровождения уголовного процесса на всех его стадиях.

При этом можно выделить следующие перспективы применения ИКТ при организации и производстве следственных и процессуальных действий:

– технология видеоконференц-связи – может составить научно-техническую основу дистанционного проведения ряда следственных действий (допроса, очной ставки, предъявления для опознания, освидетельствования);

– электронная почта – может применяться для организации ознакомления участников расследования с материалами уголовного дела в необходимом объеме; для направления заявлений, жалоб, ходатайств в адрес следователя (руководителя следственного органа) и последующего уведомления о результатах их рассмотрения; для обеспечения явки участников к следователю;

– IP-телефония – может применяться для получения следователем консультации специалиста на предмет постановки вопросов эксперту; для обеспечения права подозреваемого или обвиняемого на получение услуг защитника. Отсюда следует вывод, что представленные достижения в области информационных средств, подлежащих внедрению в процесс расследования преступлений, на современном этапе их развития предопределили разработку методологии системного и единообразного применения ИКТ как одного из перспективных направлений криминалистической техники.

Итак, ключевыми современными проблемами ТКО являются:

- порядок использования вновь разрабатываемых научно-технических средств в уголовном судопроизводстве;

- определение вектора развития профильных научных разработок;

- увеличение потенциальной возможности удовлетворения как можно большего количества «заявок на обслуживание»;

- снижение стоимости расследования;

- сокращение длительности расследования;

- исключение вероятности осуждения невинных и оправдания преступников;

- обеспечение безопасности участников расследования.

Информационно-коммуникационные технологии как элемент технико-

криминалистического обеспечения расследования преступлений – это нормативно урегулированная система научно обоснованных и безопасных средств и методов, которые обеспечивают субъекту доказывания возможность дистанционного обнаружения, сбора, хранения, передачи и использования доказательственной и ориентирующей криминалистически значимой информации.

5. Информационно- телекоммуникационная модернизация должна осуществляться по двум направлениям.

1. Разработка информационно- телекоммуникационных технологий взаимодействия полиции и общественности, документооборота между ними и отчетности полиции перед обществом. Возможности электронных средств сегодня не используются в деятельности территориальных органов внутренних дел даже наполовину. В работе полиции применяются сети связи, глобальные спутниковые навигационные системы, справочные базы данных. Отдельные госуслуги полиции нашли свое отражение на сайте «Электронного правительства». Но существенно расширить их перечень и внедрить их в полной мере в свою практику пока мешает множество проблем технического характера: отсутствие понятной всем гражданам методики доступа к порталу госуслуг; отсутствие специализированного программного обеспечения для использования этих возможностей в конкретном территориальном органе внутренних дел; отсутствие желания у сотрудников полиции кардинально менять свою работу; и т.д.

Все это приводит к слабому спросу на государственные и муниципальные услуги со стороны населения. Выход из создавшейся ситуации видится нам в повышении доступности гражданам услуг портала «Электронного правительства», расширении его функций за счет перевода всего документооборота между гражданами и полицией в электронную безбумажную форму.

Основным инструментом электронного приема обращений от граждан наряду с Интернет- обращениями должны выступать электронные терминалы–

аппаратно-программные комплексы, предназначенные для подачи обращений гражданами, предоставления справочной информации, оснащенные сенсорным экраном и специальным программным обеспечением.

2. Разработка информационно-телекоммуникационных технологий оценки деятельности полиции населением и сокращения возможностей нарушать права граждан сотрудниками полиции. Инструментом оценки качества работы сотрудников полиции с гражданами может выступать все тот же электронный терминал.

Таким образом, терминал будет служить многофункциональным устройством, позволяющим гражданам:

- подавать обращения в органы внутренних дел без участия сотрудников полиции и получать документ, подтверждающий их принятие с указанием номера, времени и даты;

- проходить самостоятельную регистрацию для входа на территорию отдела полиции, получать электронный пропуск с возможностью последующей оценки работы полицейского.

6. Эффективная борьба с преступностью зависит от уровня организации следственной, оперативной, профилактической работы, проводимой сотрудниками органов министерства внутренних дел (ОМВД). Результат такой работы будет зависеть от качества информационной поддержки, так как основные усилия сотрудников органов внутренних дел (ОВД) в предотвращении, раскрытии и расследовании преступлений связаны с получением информации. Именно данные функции и должна обеспечивать система информационного обеспечения ОВД.

Сейчас большинство региональных ОМВД России используют современные информационные системы в своей деятельности. Используемые системы могут иметь собственный язык управления данными, свои форматы и потоки данных, свои решения в части выбора технических средств и архитектуры. Использование такого подхода может сделать невозможным в будущем реализацию единого информационного пространства. Очевидна

необходимость в разработке и использовании единой информационной системы обслуживания массового пользователя.

Такой единой информационной системой может являться программная среда UTSPolice, которая предназначена для информирования граждан о деятельности ОМВД; обработки электронных обращений (сообщений) граждан и предоставление информации об услугах (контакты, обратная связь, справка, добровольная дактилоскопическая экспертиза и т.п.); отображений фотографий лиц, находящихся в розыске и т.д. В системе UTSPolice обратная связь реализована следующим образом: любой гость, через Интернет, может записаться на прием к руководителям ОМВД (выбрав сотрудника, время, свободную дату посещения и получив возможность записаться на прием, система запрашивает контактный телефон для обратной связи).

7. Диапазон правонарушений, которые выявляются с использованием Интернета, достаточно велик. Преступник, находящийся в розыске, может пользоваться социальными сетями («Одноклассники», «Facebook», «Vkontakte» и др.) и обсуждать там ограбление банка или заказное убийство. В этом случае сотруднику полиции для определения информации о преступники (номер сотового телефона, IP-адрес компьютера, переписка) необходимо направить официальный запрос в техническую поддержку социальной сети, предварительно написав им сообщение в сети Интернет.

Таким образом, использование информационных систем и социальных сетей для получении информации о преступнике, в силу стремительного развития информационных технологий, становится все более актуальным и требует дальнейшего развития и изучения. Система UTSPolice значительно упрощает взаимосвязь между гражданином и территориальным органом. Кроме того, использование подобных систем службами собственной безопасности ОМВД органов может помочь в выявлении нарушений среди личного состава служащих.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Конституция Российской Федерации // Рос. газ. – 1993. – 10 нояб.

2. Гражданский кодекс РФ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

3. Гражданский процессуальный кодекс Российской Федерации // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532.

4. Кодекс Российской Федерации об административных правонарушениях // Собрание законодательства РФ. – 2002. – № 1 (ч. I). – Ст. 1.

5. Уголовный кодекс Российской Федерации // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

6. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31 мая 2001 г. № 73-ФЗ // Собрание законодательства РФ. – 2001. – № 23. – Ст. 2291.163 1.

7. О полиции: федер. закон от 7 февраля 2011 г. № 3-ФЗ // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

8. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 21.07.2014) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

9. Об электронной подписи : федер. закон от 6 апреля 2011 г. № 63-ФЗ // Собрание законодательства РФ. – 2011. – № 15. – Ст. 2036.

10. Об организации представления государственных муниципальных услуг: федер. закон от 27.07.2010 г. №201-ФЗ (в ред. от 13.07.2015) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

11. О порядке рассмотрения обращений граждан Российской Федерации: федер. закон от 02.05.2006 г. №59-ФЗ (редакции от 24.11.2014) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

12. Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации:

приказ МВД России от 12.09.2013 г. №707 (в ред. от 20.04.2015) [Электронный ресурс]. http://www.consultant.ru/ (дата обращения: 20.08.2015)

13. Приказ МВД РФ от 14.03.2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» / http://policemagazine.ru/forum/showthread.php?t=3663.

14. Приказ МВД РФ от 28 июня 2013 г. № 490 «Об утверждении Перечня информации о деятельности образовательных организаций системы МВД России для размещения в открытых информационно-телекоммуникационных сетях, в том числе на официальном сайте МВД России в информационно-телекоммуникационной сети «Интернет», а также Порядка размещения этой информации». http://www.garant.ru/products/ipo/prime/doc/70359132/

15. Приказ Федеральной службы по надзору в сфере образования и науки от 29 мая 2014 г. № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации». http://www.rg.ru/2014/08/21/rosobrnadzor-dok.html

16. Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры» [Электронный ресурс]: Приказ МВД России от 16 января 2012 г. № 25. Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: Приказ МВД России от 6 июля 2012 г. № 678 // Рос. газ. 2012. 5 окт. № 230.

18. О внесении изменений в Указ Президента Российской Федерации от 5 мая 2014 г. №300 (О некоторых вопросах Министерства внутренних дел Российской Федерации): Указ Президента Российской Федерации от 13.июля

2015 г. №356 [Электронный ресурс]. http://publication.pravo.gov.ru (дата обращения: 22.08.2015 г.)

Материалы юридической практки

19. Апелляционное определение Московского городского суда от 20.03.2013 по делу № 10-907// СПС ГАРАНТ

20. Определение КС РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда г. Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля

21. Определение от 12.11.2007 № 12-О-07-22// СПС ГАРАНТ

22. Постановление КС РФ от 20.07.2012 № 20-П «По делу о проверке конституционности положений части первой статьи 125 и части первой статьи 152 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой гражданки Р. Г. Мишиной» // Российская газета. 2012. 08 авг.

23. Кассационное определение от 24.10.2012 по делу № 22-14391/2012// СПС ГАРАНТ

24. Кассационное определение от 31.10.2012 по делу № 22-14801/12// СПС ГАРАНТ

Монографии, публикации, учебная литература

25. Архипова Н. А. Об использовании SMS-сообщений в ходе раскрытия и расследования преступлений // Вестник Санкт-Петербургского университета МВД России. 2015. № 4 (48). С. 55.

26. Бахтеев Д. В. Уровни (стандарты) доказывания как этапы перехода от вероятности к достоверности информации / Д. В. Бахтеев // Рос. юрид. журнал. – 2014. – № 3. – С.7-10.

27. Ваулина Т.Н. Преступления в сфере компьютерной информации // Уголовное право / отв. ред. И.Я. Козаченко и др. – М.: ИНФРА-М-НОРМА, 2016. – С. 559.

28. Внуков В. И. Методы обучения ситуационному моделированию на предварительном следствии / В. И. Внуков, Юе Чжун, И. Лю // Вестник

Волгоградской академии МВД России. – 2013. – № 3. – С.41-44.

29. Волынский А. Ф. Судебно-экспертная и технико-криминалистическая – разные виды деятельности / А. Ф. Волынский, С. С. Чегодаева, В. Ю. Ткач // Вестник криминалистики. – 2013. – № 2. – С.18-23.

30. Грошиков В. А. Использование информационных технологий в раскрытии тяжких преступлений / В. А. Грошиков // Вестник Волгоградской академии МВД России. – 2014. – № 1. – С. 39-42.

31. Гуценко К.Ф., Ковалев М.А. Правоохранительные органы. Учебник для юридических вузов и факультетов. Изд. 8-е,перераб. и доп/Под ред. К.Ф. Гуценко. М.: Издательство Зеркало-М,2016. -416 с.

32. Зайцева, Е. А. Формирование доказательств следователем с использованием специальных познаний и научно-технических средств / Е. А. Зайцева, А. И. Садовский. – Волгоград, ВА МВД России, 2013. – 292 с.

33. Земцова С. И. Структура специальных знаний как предмет научной дискуссии / С. И. Земцова, В. В. Зырянов // Вестник криминалистики. – 2013. – № 1. – С. 51-55.

34. Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности : сборник научных статей / редкол. : Л. Д. Матросова [и др.]. – Орел : Орловский юридический институт МВД России имени В. В. Лукьянова, 2016. – 100 с.

35. Казначей И. В. Особенности использования технических средств коммуникации при производстве оперативно-разыскных мероприятий / И. В. Казначей // Вестник Волгоградской академии МВД России. – 2013. – № 4. - С. 59-63.

36. Карминский А.М., Оленев Н.И., Примак А.Г., Фалько С.Г. Информация в бизнесе. Методологические и практические основы построения информационной системы в организациях. – М.: Финансы и статистика, 2015. - 42 с.

37. Касаев И.Х. Совершенствование деятельности органов внутренних дел по предупреждению преступлений, совершаемых участниками этнических

преступных группировок // Уголовная политика России на современном этапе: состояние, тенденции и перспективы: сб. науч. ст. Москва: Академия управления МВД России, 2012. С. 198 – 203.

38. Кирин В.И., Минаев В.А. Информатика в деятельности органов внутренних дел: Учеб. пособие. М., 2011.

39. Колотушкин С. М. Теоретические основы идентификации человека по изображению его зубов в фото- и видеоматериалах / С. М. Колотушкин // Актуальные проблемы уголовного права и криминологии, уголовного процесса и криминалистики, уголовно-исполнительного права, преподавания учебных дисциплин криминологического цикла: Материалы международной научно-практической конференции, посвященной 20-летию образования юридического факультета (19, 20 мая 2014 г.) / отв. ред. Г. И. Цепляева. — Петрозаводск : Изд-во ПетрГУ, 2014. — С. 75-79.

40. Лавров В.П. К вопросу о соотношении криминалистики и организации расследования преступлений / В.П. Лавров // В сборнике: Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью Всероссийская научно-практическая конференция. - Орловский юридический институт МВД России имени В.В. Лукьянова; Редколлегия: А.В. Булыжкин и др.. 2015. - С. 226-232.

41. Леднев К. Ю. ИСОД МВД России и основной элемент инфраструктуры – ЕИС ЦОД // Информационные технологии, связь и защита информации МВД России. 2012. № 1. С. 25–27.

42. Лихолетов А. А. Информационно-коммуникационные технологии в системе технико-криминалистического обеспечения расследования преступлений // Роль правовой науки в развитии общества : сб. ст. междунар. науч.-практ. конф. / отв. ред. А. А. Сукиасян. – Уфа, 2014. – С.29-33.

43. Логиновский О.В., Максимов А.А. Основные положения решения задач информатизации правоохранительных органов// Международные системы – 2015.-№ 4.

44. Мельников Д. А. Информационная безопасность открытых систем. М.: Наука, 2013. 448 с.

45. Миленин Ю.Н. Проблемы допустимости применения научно- технических средств в уголовном процессе России / Ю.Н. Миленин // Юридическое лицо как субъект гражданско-правовой и уголовной ответственности и обеспечение ГИБДД условий реализации отдельных видов ответственности: сборник статей / Редкол.: Гришин А.В. - Орел: ОрЮИ МВД России им. В.В. Лукьянова, 2013. - С. 112-119.

46. Мингес И. А. Современная правовая система России: направления развития / И. А. Мингес // Вестник Волгоградской академии МВД России. – 2013. – № 4. – С.69-74.

47. Михед А.Д., Безгубова А.А. Использование правоохранительными органами интернета и телекоммуникационных систем для получения информации о криминальном событии. / Известия ТулГУ. Экономические и юридические науки. Вып. 3. Ч. II. – Тула: Изд-во ТулГУ, 2015. - С. 146-150.

48. Об организации расследования преступлений, связанных с хищением средств сотовой связи: Методические рекомендации. Волгоград, 2015. С. 5.

49. Обухова Л. А., Толстых О. В. Формализация задачи оценки защищенности информации в системах специального назначения // Процессы информационного обмена в деятельности правоохранительных органов: современное состояние и перспективы совершенствования: сборник научных статей / под ред. Л. Д. Матросовой и др. Орел, 2015. С. 14–19.

50. Орлянская Н.П., Нагоев А.В. Проблемы проектирования и внедрения информационной системы // Научный электронный журнал КубГАУ . № 01(9), 2014.- 18 с.

51. Примакин А. И., Муравьев А. В., Селюгина С. В. Использование автоматизированных рабочих мест в деятельности органов и учреждений Министерства внутренних дел Российской Федерации // Вестник Санкт-Петербургского университета МВД России. 2011. Т. 52. № 4. С. 95–99.

52. Решетняк В. И. Видеоконференц-связь в судебных стадиях уголовного

судопроизводства // Перспективы развития уголовно- процессуального права и криминалистики: материалы II междунар.-практ. конф., Москва, 11–12 апреля 2012 г. М., 2012. С.11-15.

53. Семененко Г.М. О применение географических информационных систем в деятельности органов внутренних дел по предупреждению преступлений //Сборник научных трудов «Проблемы борьбы с преступностью Российский и международный опыт». Вып. 4. Волгоград. 2014. С. 89 – 94.

54. Семененко Г.М., Герасимов К.Е. Об исторических аспектах развития географических информационных систем в России и зарубежо» // Эволюция современной наук: сб. статей международной научно-практической конференции. Уфа. 2015. С. 182 – 186.

55. Семенов Е. Ю. АРМ сотрудника ДПС на основе планшетного компьютера // Наука и практика. 2015. № 2 (63). С. 168–170.

56. Шапошников А. Ю. Ходатайство о получении информации об абонентах должно быть обоснованным // Уголовный процесс. 2016. № 10. С. 43.

Электронные ресурсы

57. Выступление Председателя правительства Российской Федерации Д.А. Медведева по итогам совещания «О развитии сети многофункциональных центров по предоставлению государственных и муниципальных услуг», состоявшегося 18 января 2013 г. [Электронный ресурс]. http://www.government.ru (дата обращения: 20.08.2015)

58. Гуев А. Н. Постатейный комментарий к Уголовно-процессуальному кодексу Российской Федерации [Электронный ресурс], Доступ из СПС «Гарант», 2016.

59. Использование программно-аппаратного комплекса для оказания электронных услуг населению [Электронный ресурс]. – Режим доступа: http://www.ormvd.ru/pubs/102/15612/ (Дата обращения: 18.06.2017).

60. Полиция в социальной сети. Newsland. [Электронный ресурс]. – Режим доступа: http://newsland.com/ (Дата обращения: 18.06.2017).

61. Предполагаемых убийц астраханки выдал сотовый телефон // ИА REGNUM [Электронный ресурс]. URL: www.regnum.ru (дата обращения: 06.06.2017).

62. Путин В.В. Демократия и качество государства [Электронный ресурс]. http://www.kommersant.ru (дата обращения: 22.08.2015)

63. Управление «К» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Управление_К (Дата обращения: 18.06.2017).