

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Юридический институт
Кафедра «Правоохранительная деятельность и национальная безопасность»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
« ____ » _____ 2019 г.

**Информационные технологии как средство повышения эффективности
организации правоохранительной деятельности**

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ФГАОУ ВО «ЮУрГУ» (НИУ)–40.05.02.2019.290. ВКР

Руководитель работы
« ____ » _____ 2019 г.

Автор работы
« ____ » _____ 2019 г.

Нормоконтролер

« ____ » _____ 2019 г.

Челябинск 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
1 ТЕОРЕТИЧЕСКИЕ И ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	7
1.1 Понятие и содержание информационных технологий, используемых в правоохранительной деятельности	7
1.2 Современное состояние и основные направления использования информационных технологий в правоохранительной деятельности	14
1.3 Правовое регулирование применения информационных технологий в правоохранительной деятельности	26
2 ПЕРСПЕКТИВЫ РАЗВИТИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	35
2.1 Информационное обеспечение раскрытия и расследования преступлений с помощью компьютерной техники	35
2.2 Использование сети Интернет для решения задач по раскрытию преступлений	40
2.3 Совершенствование информационных технологий в правоохранительной деятельности	46
ЗАКЛЮЧЕНИЕ	51
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	54
Приложение 1	60
Приложение 2	62

ВВЕДЕНИЕ

На сегодняшний день цифровизация становится основным показателем прогрессивного развития любого государства. По данным международного рейтинга конкурентоспособности государств в цифровой среде – World Digital Competitiveness Ranking, Россия в 2018 году заняла 45 место из 63 стран. По сравнению с 2017 годом показатель улучшился всего на одну позицию, обогнав таким образом Филиппины¹. Итоговая рейтинговая система рассчитывается на основе трех показателей: качество образования и науки («Знания»); регуляторная среда, финансовый капитал в IT-отрасли, состояние интернета и коммуникационных технологий («Технологии»); уровень готовности использования цифровой трансформации («Будущая готовность»).

По данным международного рейтинга развития информационно-коммуникационных технологий – ICT Development Index (IDI), в 2018 году Российская Федерация занимает 45 позицию среди 176 стран, в то время как в 2017 году она занимала 43 место². Тем самым на сегодняшний день мы уступаем Португалии и Уругваю. Международный рейтинг развития ИКТ определяет показатели, значение которых необходимо улучшить для сокращения «цифрового разрыва» с наиболее развитыми странами. Основными показателями являются: доступность к ИКТ; использование ИКТ; навыки использования ИКТ. Важно отметить, что место России в данном рейтинге входит в число контрольных показателей Стратегии развития информационного общества в Российской Федерации и государственной программы «Информационное общество (2011 – 2020 годы)».

¹ IMD World Competitiveness Center. URL:<https://www.imd.org/globalassets/wcc/docs/release-2018/ranking2018.pdf>

² International Telecommunication Union. URL:<https://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017rank-tab>

Таким образом, цифровизация является существенным показателем развития любого государства. На сегодняшний день наше государство стремится начать новый этап формирования информационного общества. Происходит переход от внедрения информационных технологий к комплексному построению цифровой системы в масштабах всей страны. В соответствии с этим была разработана национальная программа «Цифровая экономика Российской Федерации» на 2018-2024 гг., утвержденная распоряжением Правительства РФ от 28 июля 2017 г. №1632-р.

Безусловно правоохранительная деятельность не может оставаться в стороне. Государство стремится использовать достижения науки и техники, чтобы идти в ногу с преступностью и даже опережать ее, обеспечивая таким образом законность и правопорядок. Появление новых информационных технологий в правоохранительных органах, цифровизация правоохранительной деятельности – это качественный прорыв в обеспечении правопорядка в нашей стране.

Необходимость изучения проблем внедрения и развития информационных технологий в правоохранительную деятельность обусловлена тем, что политика государства в сфере информатизации является одной из ведущих на сегодняшний день направлений политики российского государства.

Использование информационных технологий в правоохранительной деятельности необходимо, в первую очередь, для упрощения работы и повышения её оперативности, а во-вторых, для обеспечения эффективной борьбы с преступностью. Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы, проводимой правоохранительными органами. Естественно, результаты данной работы зависят от уровня информационной поддержки, развития информационных технологий и их полного внедрения в правоохранительные органы, обеспечения доступа сотрудникам к использованию информационных технологий при любом необходимом

случае, связанным с профессиональной деятельностью. Прежде всего, это объясняется тем, что, специалисту приходится работать с огромным информационным потоком социально-правовой информации, справиться с которыми без технических и программных средств практически невозможно.

Данные положения обуславливают актуальность темы исследования.

Отдельные вопросы проблем информатизации правоохранительной деятельности освещались в работах С.В. Баженова, С.И. Грицаева, А.И. Жукова, С.В. Зуева, Е.В. Никитина, В.В. Помазанова и некоторых других авторов.

Объектом исследования выпускной квалификационной работы являются общественные отношения, складывающиеся в процессе использования информационных технологий в правоохранительной деятельности.

Предметом исследования являются нормы международного и российского законодательства, посвященные информационным технологиям в правоохранительной деятельности, а также правоприменительная практика.

Целью исследования, проведенного в выпускной квалификационной работе, является поиск оптимальных путей повышения эффективности использования информационных технологий в правоохранительной деятельности, правового регулирования отношений, возникающих в процессе использования информационных технологий, и выработка практических рекомендаций по облегчению внедрения информационных технологий в правоохранительную деятельность.

Для достижения поставленной цели необходимо решить следующие задачи:

- дать оценку современного состояния информационных технологий в правоохранительной деятельности
- произвести анализ направлений развития информационных технологий в правоохранительной деятельности;

- изучить действующее законодательства в сфере применения информационных технологий в правоохранительной деятельности;
- ознакомиться с использованием компьютерной техники, используемой в целях информационного обеспечения раскрытия и расследования преступлений;
- определить значение сети Интернет для решения задач по раскрытию и расследованию преступлений;
- выявление недостатков и пробелов в регулировании общественных отношений, складывающихся в процессе применения информационных технологий в правоохранительной деятельности;
- выработка предложений по совершенствованию и развитию информационных технологий в правоохранительной деятельности.

В качестве методологической основы исследования применялись научные методы: историко-сравнительный, анализа, системный, формально-логический, сравнительно-правовой, анкетирования и др.

Научно-теоретическую базу выпускной квалификационной работы составляют труды известных ученых: Н.Д. Андреев, Р.С. Белкин, Л.Н. Демидов, К.О. Сливинский, В.Ю. Толстолицкий, А.С. Шаталов и др.

В работе освещено понятие информационных технологий в правоохранительной деятельности, описано их состояние на сегодняшний день, рассмотрены перспективы развития, а также выявлен ряд проблем и предложены пути решения. Результаты работы имеют практическую значимость, содержат выводы и предложения автора по проблемам, связанных с использованием информационных технологий в правоохранительной деятельности.

Структура выпускной квалификационной работы состоит из введения, двух глав, разделенных на параграфы, заключения, библиографического списка и четырех приложений.

1 ТЕОРЕТИЧЕСКИЕ И ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

1.1 Понятие и содержание информационных технологий, используемых в правоохранительной деятельности

Правоохранительную деятельность в Российской Федерации осуществляют правоохранительные органы. Информация, используемая в правоохранительной деятельности, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории правоохранительных органов, о самих органах и подразделениях, их силах и средствах.

Следует отметить, что информационное обеспечение органов внутренних дел является одним из наиболее приоритетных направлений развития правоохранительной системы. Так, 28 мая 2019 года председатель правительства Дмитрий Медведев заявил о необходимости модернизации технической инфраструктуры МВД на заседании прав комиссии по цифровому развитию, использованию ИТ для улучшения качества жизни и условий ведения предпринимательской деятельности. По его словам, это необходимо для эффективной работы информационных систем МВД¹.

Успешное функционирование информационного обеспечения правоохранительных органов во многом зависит от современных информационных технологий, способных оказать действенную помощь в выявлении, предупреждении и раскрытии преступлений.

Развитие информационных технологий, по мнению И. Л. Коноплевой, О. А. Хохловой, А. В. Денисова, можно разделить на эволюционные этапы²:

¹ Информационные технологии в МВД России: Официальный сайт МВД России. URL: <http://www.tadviser.ru/index.php/>

² Информационные технологии: Уч. пособие / под. ред. И.Л. Коноплевой. – М., 2009. – С. 15

- 1 этап – возникновение человеческой речи;
- 2 этап – появление письменности;
- 3 этап – распространение книгопечатания (XV в.);
- 4 этап – изобретение и распространение средств передачи информации: радио, телефона, телеграфа (конец XIX – начало XX в.);
- 5 этап – изобретение и распространение телевидения и электронно-вычислительных машин (середина XX в.);
- 6 этап – изобретение микропроцессоров, создание персональных компьютеров (вторая половина XX – начало XXI в.);

Развитие информационных технологий в правоохранительной деятельности, по нашему мнению, должно рассматриваться с момента появления первых ЭВМ в правоохранительных органах.

Так, в 1968 году происходит компьютеризация деятельности информационных подразделений МВД СССР, благодаря чему коренным образом изменилась их практическая деятельность по информационному обеспечению органов внутренних дел. А также создается информационно-вычислительный центр (ИВЦ) МВД СССР с целью совершенствования информационного обеспечения центрального аппарата министерства для решения задач по комплексной автоматизации учетно-вычислительных работ.

Для совершенствования современной информационной службы МВД России судьбоносным поворотом стал приказ Министра внутренних дел СССР от 9 ноября 1970 г. «Об организации Главного информационного центра при МВД СССР». Главный информационный центр (ГИЦ) был создан «в целях улучшения системы сбора и обработки информации и использования ее в оперативно-служебной деятельности МВД СССР». Тогда же началось создание информационных центров по всей стране.

Главный информационный центр выполнял следующие основные задачи: организация системы машинной обработки специальной информации; исследование процессов управления в отрасли и

совершенствование этих процессов на базе комплексного применения современных организационных форм управления, математических методов, вычислительной техники и средств связи; разработка и внедрение отраслевой автоматизированной системы управления в сфере деятельности МВД СССР.

Началась разработка автоматизированных информационно-поисковых систем различного назначения. Впервые в истории органов внутренних дел приступили к решению задач по их компьютеризации.

С появлением компьютеров, способных за доли секунд обрабатывать тысячи однородных записей, время картотечных шкафов, заполненных тысячами бумажных карточек, закончилось.

В 80-х годах внедрение персональных электронно-вычислительных машин в деятельность органов внутренних дел, внедрение системы теледоступа с использованием мультипроцессоров позволили приступить к созданию информационно-вычислительных сетей. Этот процесс был очень важным, потому что максимально приблизил к работникам системы хранения и обработки информации, позволил создавать локальные сети и автоматизированные рабочие места (АРМ).

Современный этап применения современных информационных технологий в правоохранительных органах связан с принятием в 1993 году Концепции развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью. Она стала основой осуществления единой научно-технической политики в области компьютеризации, создания информационно-вычислительных сетей (ИВС) и средств связи, внедрения новейших информационных технологий и создания объединенных баз данных различного уровня.

XXI век ознаменовался переходом всей информационной службы органов внутренних дел на более высокий качественный уровень своего развития – формирование инфраструктуры единого информационного пространства МВД России на основе интеграции информационных ресурсов.

В 2002 году ГИЦ МВД России разработана Концепция развития информационно-вычислительной системы МВД России на 2002-2006 годы¹. Целью концепции явилось повышение эффективности использования существующих в МВД России информационных ресурсов в обеспечении развития ИВС как системы, интегрирующей информационные массивы органов внутренних дел на основе перспективных технологий их обработки.

Реформирование системы Министерства внутренних дел России в 2011 году дало толчок в совершенствовании данной структуры в области информационных технологий. Был принят новый Федеральный Закон, регулирующий деятельность полиции. В нем появилась статья, затрагивающая применение информационных технологий в деятельности полиции, которой в Законе РФ «О милиции» не было. Так, в соответствии со ст. 11 Федерального Закона «О полиции», сотрудник полиции «в своей деятельности обязан использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру». Также в 2011 году в рамках реформы в составе МВД России был создан новый специализированный Департамент информационных технологий связи и защиты информации, который призван решать задачи внедрения «самых современных технологий управления»².

Повсеместное использование информационных технологий имело своей целью повышение эффективности деятельности не только МВД России, но и другие правоохранительные органы. В связи с этим стали вводиться новейшие информационные технологии: Автоматизированные рабочие места (АРМ): следователя, прокурора, оперативного работника и т.д., портативные устройства типа «Кейс-КПМ» и «Терминал-ТМ-5», Единая

¹ Приказ МВД России от 13 июня 2002 г. № 562 «Об утверждении Концепции развития информационно-вычислительной системы МВД России на 2002-2006 годы». URL: <https://base.garant.ru/1353176>

² Образован Департамент информационных технологий, связи и защиты информации МВД России: Официальный сайт МВД России. URL: <https://мвд.рф/news/item/172419>

информационно-телекоммуникационная сеть органов внутренних дел (ЕИТКС ОВД) и других правоохранительных органов, предоставление доступа в сеть Интернет для всех правоохранительных органов, Аппаратно-программный комплекс (АПК) «Безопасный город» и множество других.¹

Технология – последовательность действий, совершаемых над предметом труда в целях получения конечного продукта.

Термин «информационная технология» среди ученых в области информатики определяется как совокупность средств и методов по сбору, хранению, накоплению, поиску и обработке информации с помощью средств вычислительной техники. Особенностью информационной технологии является то, что предметом и продуктом труда является информация, а орудием труда – вычислительная техника и средства связи. Цель информационных технологий – производство информации для анализа человеком и принятии на его основе решения по выполнению какого-либо действия (управленческого решения).²

Следует отличать понятия «информационная технология» и «информационная техника». Последняя представляет собой материальную основу информационной технологии, с помощью которой осуществляется сбор, хранение, передача и обработка информации³. То есть, информационная техника входит в информационную технологию, как часть и целое. Информационная техника только в совокупности со специальным программным обеспечением, методами их использования может решать задачи правоохранительной деятельности. Данная совокупность составляет информационную технологию.

Информатизация современного общества стремительно приближается к своему абсолютному значению: большая часть жителей развитых стран являются активными пользователями компьютерной техники, имеющей

¹Цимбал В.Н. Некоторые вопросы использования сотрудниками полиции информационных технологий // Общество и право. – 2015. – №1 (51). – С. 233.

²Демидова Л.Н. Информационные технологии. – М., 2017. – С. 16.

³Артамонов Б.Н. Основы современных компьютерных технологий. – СПб., 2002. – С. 12.

возможность выхода в Интернет. Для регулирования общественных отношений, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении ИТ и обеспечении защиты информации Государственной думой был принят Федеральный Закон от 27. 07. 2006 г. № 149 – ФЗ «Об информации, информационных технологиях и о защите информации». В ст. 2 даны следующие интересующие нас основные понятия:

– информация – сведения (сообщения, данные) независимо от формы их представления;

– информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

– информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

– информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием вычислительной техники.

Данные определения являются общими, подходящими практически для любой сферы деятельности современного человека. Для того, чтобы дать более узкое понятие информационным технологиям, которые будут затрагивать правоохранительную деятельность, нами представляется необходимым рассмотреть сущность и направления правоохранительных органов.

Правоохранительные органы – обособленная группа государственных органов, осуществляющая деятельность по охране правопорядка и законности, защите прав и свобод человека.

Все правоохранительные органы осуществляют одну или несколько из следующих функций:

– конституционный контроль;

- прокурорский надзор;
- расследование правонарушений;
- обеспечение безопасности;
- исполнение судебных решений;
- оперативно-розыскная деятельность;
- охрана общественного порядка;
- оказание юридической помощи;
- профилактическая деятельность.

Для обеспечения каждой функции существуют свои специфические задачи, которые призваны выполнять конкретный правоохранительный орган. Соответственно использование информационных технологий должно быть направлено на эффективное выполнение поставленных задач. К тому же в состав любого правоохранительного органа, наряду с подразделениями, непосредственно занимающимися решением конкретных правоохранительных задач, входят иные подразделения и службы, призванные обеспечивать и координировать их работу (финансовые, кадровые и другие).

Следовательно, информационные технологии должны обеспечивать каждую из видов правоохранительной деятельности: как при расследовании, раскрытии и предупреждении преступлений и правонарушений, так и в управленческой и, так называемой, офисной работе.

Таким образом, информационные технологии, используемые в правоохранительной деятельности – это совокупность методов, производственных процессов, программно-технических средств, объединенных в технологическую цепочку, обеспечивающих сбор, хранение, обработку, передачу правоохранительной информации, а также использующихся в целях управления, автоматизации всех офисных, канцелярских работ, утверждения решений и работоспособности экспертных систем.

1.2 Современное состояние и основные направления использования информационных технологий в правоохранительной деятельности

В настоящее время использование информационных технологий стало одним из факторов успешной деятельности правоохранительных органов в поддержании правопорядка, защите прав, свобод и законных интересов граждан, расследовании и раскрытии правонарушений и преступлений и отправлении правосудия.

Проанализируем главные направления информационных технологий в правоохранительной деятельности, рассмотрев их использование в основных правоохранительных органах.

Информационные технологии в ОВД.

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах.

В современных условиях составной частью криминалистического обеспечения раскрытия и расследования преступлений является информационное обеспечение этой деятельности, поскольку сущность расследования преступлений – это поиск информации и работа с ней.

Информационное обеспечение представляет собой процесс с определенными, последовательно сменяющимися друг друга стадиями, в котором субъекты воздействуют на объекты (информацию) для достижения конкретных результатов (целей). Процесс информационного обеспечения начинается с получения криминалистически значимой информации от ее источника или потенциального носителя.

В информационном обеспечении органов внутренних дел центральное место занимают учеты, которые используются для регистрации первичной информации о преступлениях и лицах, их совершивших. Учет – это система

регистрации и хранения информации о лицах, совершивших преступления, о самих преступлениях и связанных с ними фактах и предметах.

Учеты ОВД ведутся по двум направлениям: по линии главного информационного центра (ГИЦ МВД России) и экспертно-криминалистического центра (ЭКЦ МВД России). Далее разбиваясь на региональные и местные центры. Таким образом первоначальный сбор и хранение криминальной информации начинается с горрайлинорганов МВД России.

Главный информационный центр (ГИЦ) – самый крупный банк оперативно-справочной и розыскной информации в системе МВД России. На него возложена задача обеспечения органов и учреждений внутренних дел различной информацией – статистической, розыскной, оперативно-справочной, криминалистической, производственно-экономической, научно-технической, архивной.

Экспертно-криминалистический центр (ЭКЦ) МВД России хранит в себе экспертно-криминалистические централизованные коллекции и картотеки.

Значение совершенствования информационных технологий в системе учетов деятельности ОВД по раскрытию и расследованию преступлений играет немаловажную роль. Так, если в 1976 г. с помощью криминалистических, розыскных оперативно-справочных учетов было раскрыто 4% от общего числа раскрытых преступлений, в 1996 г. – 25, в 1999 г. – 43, в 2002 г. – 60%, то в последние годы с помощью информационных технологий раскрыто более 80%. Общий объем централизованных криминалистических, розыскных и специализированных информационных массивов составил около 230 млн. объектов учета¹.

Учеты органов внутренних дел в зависимости от способа обработки информации подразделяются на три вида: ручные, механизированные и автоматизированные.

¹ Пресс-служба ГИАЦ МВД России: сайт. URL: <http://www/mvd/tu/news/31439>

Автоматизированные учеты состоят из ряда автоматизированных информационно-поисковых систем (АИПС). Примерами могут служить:

- АИС «РОЗЫСК ЛИЦ РФ» – автоматизированная информационная система учета лиц, находящихся в федеральном розыске;
- АИС «ОРУЖИЕ» – автоматизированная информационная система учета владельцев огнестрельного оружия;
- АБД «АНТИКВАРИАТ» – автоматизированная база данных учета антиквариата¹ и т.д.

Рассмотрим преимущество информационных систем на примере автоматизированной дактилоскопической информационной системы (АДИС «Папилон»). Данная система создана с целью автоматизированной обработки данных, полученных в ходе государственной дактилоскопической регистрации, а также экспертно-криминалистического учета следов рук. АДИС «Папилон» существует в системе МВД России на федеральном, межрегиональном и региональном уровнях².

Обратим внимание на способы фиксации биометрической информации. Фиксация биометрической информации осуществляется различными способами, такими как:

- копирование бумажной дактилокарты при помощи планшетного сканера;
- создание электронной дактилокарты на основе метода бескраскового дактилоскопирования биометрической информации в Папилон «Живой сканер» и мгновенный экспорт полученной дактилокарты в АДИС «Папилон»;
- ввод дактилоскопической информации из электронных фотографий.

¹ Андреев Н.Д. Современные системы информационного обеспечения сотрудников ОВД: монография. – Уфа, 2008. – С. 50–51.

² Реализованные проекты АДИС "Папилон" в МВД России. URL: <http://www.papilon.ru/rus/20/>

Благодаря созданию данной информационной технологии использование биометрических материалов перешло на качественно новый уровень. Так, математическая модель поиска берет во внимание топологические характеристики гребневой структуры папиллярного узора, что в свою очередь является самым точным сравнительным показателем¹. А также увеличилась скорость по поиску лица, которому принадлежат полученные образцы, поскольку автоматический поиск системы «Папилон» меньше чем за минуту выдает рекомендательный список биометрических образцов.

Так, приговором № 1-648/2016 от 25 октября 2016 г. по делу № 1-648/2016 Калининский районный суд г. Челябинска признал виновным гр. Ч. по ч.1. ст. 105 УК РФ и судом установлено, что гр. Ч. совершил убийство при следующих обстоятельствах. В период времени с 13 часов по 19 часов 26 минут на участке местности между находившимися в состоянии алкогольного опьянения гр.Ч. и гр. Н. произошел конфликт, в ходе которого у гр. Ч. из личной неприязни возник преступный умысел на убийство гр. Н. Реализуя свой преступный умысел, гр. Ч., находясь в указанное время и в указанном месте в состоянии алкогольного опьянения, осознавая и понимая, что его действия причинят смерть, и, желая этого, нанес не менее 26 ударов руками и обутыми ногами в голову гр. Н., не менее 10 ударов руками и обутыми ногами по туловищу гр. Н. и не менее 10 ударов руками и обутыми ногами по верхним и нижним конечностям гр. Н. После этого гр. Н., продолжая реализовывать свой преступный умысел, вооружился имевшимся при нем ножом и нанес им гр. Н. не менее 10 ударов в область шеи, не менее 20 ударов в область головы и не менее 2 ударов в область верхних конечностей. Указанными преступными действиями гр. Ч. причинил множество травм, которые повлекли смерть гр. Н. на месте происшествия от черепно-мозговой травмы в течение первых часов после травмы.

¹ Подробно об АДИС "Папилон": сайт. URL:<https://www.papillon.ru/rus/38?>

Согласно рапорту на имя начальника ОП Калининский г. Челябинска в 19 часов 33 минуты поступило сообщение об обнаружении трупа мужчины. Из рапорта оперуполномоченного следует, что по системе «АДИС Папилон» была установлена личность обнаруженного трупа мужчины. Суд, исследовав представленные материалы дела, приходит к выводу, что в действиях гр. Ч. имеется состав преступления, предусмотренный ч. 1 ст. 105 УК РФ. Вина его также подтверждается представленными материалами дела: справкой о результатах проверки объекта на экспертнокриминалистический учет, согласно которой дактилокарта гр. Ч., направленная эксперту на проверку, по результатам проверки с аналогичными отпечатками и оттисками в базе «АДИС Папилон» ГУ МВД России по Челябинской области установлено полное совпадение с отпечатками пальцев с данной дактилокарты¹.

Но не всегда использование информационных систем улучшает скорость и качество работы сотрудников ОВД. Как отмечалось выше сотрудники ОВД в своей деятельности пользуются такими видами учетов, как статистическими розыскными, оперативно-справочными, экспертно-криминалистическими, архивными. Однако использование оперативно-справочных учетов имеет ряд трудностей. Проблема пользования оперативно-справочными учетами кроется в четком ограничении круга должностных лиц, имеющих доступ к ним. Дело в том, что следователь, как лицо ведущее расследование преступления, не входит в перечень этих лиц. Другими словами, он не имеет право напрямую использовать данные из оперативно-справочных учетов, что, по нашему мнению, может значительно понизить качество расследования. Так, получение следователем информации из оперативно-справочных учетов поступает из от оперативных работников по их же инициативе. Понижение качества расследования в данном случае обосновывается важностью информации в ходе расследования преступления на первоначальном этапе. Например, информация из учета может

¹ Приговор Калининского районного суда г. Челябинска № 1-648/2016 от 25 октября 2016 г. по делу № 1-648/2016. Судебные и нормативные акты РФ. URL: <http://sudact.ru>

использоваться при построении версий и определении направления расследования, однако длительный процесс ее получения замедляет работу следователя. Сам следователь при расследовании преступлений используют всего около десяти учетов, таких как: учеты о наличии или отсутствии судимости, учеты лиц, пропавших без вести, учеты неопознанных трупов, учеты нераскрытых преступлений, дактилоскопический учет и т.д. Причем, как отмечают Грицаев С.И., Помазанов В.В., процесс получения следователем информации из учета излишне усложнен и очень долог¹.

С марта 2012 года в МВД России функционирует единая информационно-телекоммуникационная система (ИСОД). ИСОД – это уже вторая попытка МВД обзавестись единой информационной системой, после неудачной разработки прошлой версии – ЕИТКС, которая так и не заработала.

ИСОД представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства.

Сервисы ИСОД подразделяются на сервисы повседневной деятельности, сервисы межведомственного взаимодействия и оказания государственных услуг и сервисы оперативно-служебной деятельности.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД включают:

- 1) сервис электронного документооборота (СЭД);
- 2) сервис электронной почты (СЭП);
- 3) ведомственный информационно-справочный портал (ВИСП);
- 4) систему видеоконференцсвязи.

¹ Грицаев С.И., Помазанов В.В. Автоматизированное рабочее место следователя при производстве расследования: возможности и применение. // Российский следователь. – 2019. – №2. – С. 13

Прикладные сервисы обеспечения оперативно-служебной деятельности включают:

- информационно-поисковый сервис «Следопыт-М»;
- сервис обеспечения охраны общественного порядка (СООП);
- сервис обеспечения деятельности дежурных частей (СОДЧ);
- сервис обеспечения деятельности подразделений материальнотехнического обеспечения МВД (СОМТО);
- федеральную информационную систему ГИБДД (ГИБДД-М);
- сервис обеспечения экономической безопасности (СОЭБ); сервис НЦБ Интерпола (СОДИ);
- сервис экспертно-криминалистической деятельности (ЕАИС ЭКП);
- сервис обеспечения государственной защиты лиц (СУОГЗ);
- сервис оформления проезда сотрудников (СОПС);
- сервис ГУ собственной безопасности МВД (СОПД ГУСБ);
- сервис статистической отчетности (МОСТ);
- банк отпечатков пальцев (ЦИАДИС).

Подсистема поддержки взаимодействия с населением, а также межведомственного взаимодействия с целью предоставления госуслуг включает:

- а) сервис предоставления госуслуг (СПГУ);
- б) систему централизованного учета оружия (СЦУО);
- в) единый банк данных архивной информации (Ретроспектива);
- г) интегрированный банк данных.

Еще одним видом информационных технологий являются автоматизированные рабочие места (АРМ). Они представляют собой комплекс технических средств (ПК, принтер, средства обеспечения телефонных переговоров, факсимильной связи и т.д.) так и компьютерные

программы, решающие задачи сотрудника того или иного подразделения ОВД. Более подробно мы разберем их в следующей главе.

Среди информационных технологий, применяемых в ОВД, можно выделить средства выявления правонарушений и преступлений. К таковым относятся система видеонаблюдения. Она представляет собой аппаратно-программный комплекс, где на компьютер оператора с видеокамер непрерывно поступает видеоизображение конкретного участка местности в режиме удаленного доступа. Оператор может непрерывно проводить мониторинг участка местности, либо просматривать видеозаписи. Такие системы видеонаблюдения используются, например, для фиксации правонарушений в области дорожного движения, либо для выявления преступников или правонарушителей на улицах города, во дворах домов, а также в местах массового скопления людей, с целью предотвращения террористической угрозы и т.д.¹.

Согласно приказу МВД России от 29 января 2008 г. №81 «Об организации комплексного использования сил и средств органов внутренних дел Российской Федерации по обеспечению правопорядка в общественных местах» системы видеонаблюдения используются для решения таких задач, как:

- оценка оперативной обстановки, организационное и информационно-аналитическое обеспечение управленческих решений;
- своевременное выявление противоправных действий, организация их расследования, раскрытия и предотвращения;
- создание видеоархивов, позволяющих использовать их в качестве доказательств.

Обычно сотрудники ОВД используют записи с видеокамер, для установления конкретных событий, лиц, автотранспорта и т.д. при

¹ Смахтин Е.В., Щербич С.В. Некоторые вопросы использования систем видеонаблюдения в деятельности правоохранительных органов по раскрытию и расследованию преступлений. // Российское право: Образование. Практика. Наука. – 2017 – №6 (102). – С. 77.

расследовании преступлений. Но, как отмечают Е.В. Смахтин и С.В. Щербич, на смену видеоаналитике приходит видеосемантика. И если первая представляла собой выборку конкретных ситуаций из общего числа потока, то последняя самостоятельно обнаруживает признаки совершаемого правонарушения или преступления и предлагает оператору конкретный короткий эпизод из всего видеомассива. Это достигается путем использования метода математического анализа общего видеопотока¹. Например, такая система используется в ГИБДД при фиксации нарушителей правил дорожного движения.

В ходе мероприятий по пресечению противоправных действий положительно зарекомендовало себя использование систем мониторинга подвижных объектов на базе ГЛОНАСС в дорожно-патрульной службе, патрульно-постовой службе, охранно-конвойной службе, группах немедленного реагирования дежурных частей, группах задержания вневедомственной охраны.

Основными целями создания подобных систем является повышение эффективности взаимодействия всех функциональных и территориальных подразделений органов внутренних дел при несении службы, сокращение времени реагирования на происшествия и совершённые преступления.

В состав систем входят модули мониторинга подвижных объектов, АРМ, сервер обработки информации со специализированным ПО. Таким образом, вся навигационная информация о местоположении, скорости, направлении движения транспортных средств, а также служебная информация передается на диспетчерский пульт управления. Программное обеспечение системы обеспечивает отображение автомобилей, нарядов, оснащенных терминальными устройствами, на электронной карте местности, отслеживание их нахождения и заданных зонах патрулирования, контроль маршрутов, составление отчетов и многое другое.

¹ Там же. С. 79

Дежурный может направлять свободный и ближайший к месту происшествия мобильный экипаж. Тем самым, внедрение навигационно-мониторинговых систем обеспечивает оперативность реагирования на сигнал тревоги и позволяет своевременно предотвращать противоправные действия.

Информационные технологии Прокуратуры РФ.

В деятельности прокуратуры информатизация подразумевает под собой перевод аналоговой информации в цифровой вид для более удобной работы с ней. Разработка и внедрение информационных технологий и систем в органы прокуратуры производится с целью уменьшения в прокурорской деятельности ошибок из-за недостоверной информации, а также упрощения системы делопроизводства и повышения оперативности прокуроров в их работе¹. Единая информационная среда создается для органов прокуратуры, распределенных по всей территории России и образующих трехуровневую систему:

1 уровень - Генеральная прокуратура РФ;

2 уровень - прокуратуры республик в составе Российской Федерации; прокуратуры краев, областей, городов Москвы и Санкт-Петербурга, автономной области, автономных округов; иные территориальные прокуратуры; специализированные прокуратуры, приравненные к прокуратурам областей;

3 уровень - прокуратуры городов и районов; специализированные прокуратуры, приравненные к прокуратурам районов.

В 1992 году была разработана автоматизированная система информационного обеспечения органов прокуратуры Российской Федерации (АСИО-Прокуратура). Данная информационная система преследовала цель создания единой автоматизированной информационной среды на всей территории Российской Федерации, которая будет оперативно и

¹ Паламарчук С.А. Совершенствование конституционно-правового регулирования права на информацию в сети интернет // Северокавказский юридический вестник. – 2015. – №4. – С. 108

максимально полно удовлетворять информационные потребности всех уровней прокуратуры при осуществлении ими своих функций. Для достижения поставленной цели АСИО-Прокуратура решает следующие задачи:

- расширение анализа законности и правопорядка;
 - организация АРМ прокурора по различным направлениям деятельности;
 - увеличение скорости получения и обработки информации;
 - создание интегрированного банка данных из локальных баз данных, собранных с каждого уровня управления прокуратуры;
 - создание единой информационно-вычислительной сети;
- обеспечение информационного взаимодействия с другими государственными органами, путем внедрения электронного документооборота;
- освобождение прокуроров от рукописного труда¹.

В настоящее время в системе органов прокуратуры РФ используются информационные системы органов прокуратуры (ИСОП). ИСОП – это совокупность автоматизированных систем по различным направлениям деятельности прокуратуры. В научной литературе основными подсистемами называются:

- АИК «НАДЗОР» – информационно-документационное обеспечение надзорной деятельности на всех уровнях прокуратуры РФ;
- АИК «КАДРЫ-ОП» – учет кадров органов прокуратуры, используемая в Генеральной прокуратуре РФ и прокуратурах регионального звена;
- АРМ «Статистика» – обеспечение статистической деятельности при статистической отчетности и т.д.².

¹ Лисенкова Л.В. Влияние информационных технологий на прокуратуру // Электронный вестник Ростовского социально-экономического института. – 2017. – №2. – С. 140

² Ивлев А.Ф., Потапова И.И., Сугайпова Э.А., Елисеева Ю.А. Информационные технологии в организации прокурорского надзора // Вестник Российской академии естественных наук. – 2015. – №19. – С. 8

Современный этап развития информационных технологий в органах прокуратуры связан с созданием Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года. Проект разработан на период с января 2018 года по декабрь 2025 года. Цель: совершенствование информационного обеспечения органов и организаций прокуратуры РФ, определение основных приоритетов и принципов его развития, активизация деятельности в области информатизации¹. Паспорт проекта содержит данные о результатах проведенной работы за 2018 год:

- создан защищенный интернет через сегмент сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации (RSNET) на 3 тыс. объектов, мин. на 1 рабочем месте в каждом объекте прокуратуры;

- проведены мероприятия по организации единых защищенных автоматизированных рабочих мест (внедрены до 10 тыс. типовых рабочих мест);

- создана защищенная электронная почта органов прокуратуры Российской Федерации - у каждого работника прокуратуры настроен персональный электронный почтовый ящик (до 50 тыс. электронных почтовых ящиков);

- введение в эксплуатацию IP-телефонии (появилась возможность совершения видеозвонков и аудиоконференций);

- внедрение электронного документооборота; введен в опытную эксплуатацию модуль «Учет работы прокуроров» - государственная автоматизированная правовая статистика (ГАС ПС)².

В настоящее время использования информационных технологий имеет ряд проблем, таких как: обеспечение безопасности информационных

¹ Приказ Генерального прокурора Российской Федерации «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» от 14.09.2017 № 627 // Законность. - 2017. - №12. (Приказ)

² Паспорт проекта цифровой трансформации органов и организаций прокуратуры Российской Федерации. Официально документ опубликован не был. URL:http://d-russia.ru/wp-content/uploads/2018/02/GP_trasformatsia_plan.pdf.

правоохранительных систем; выход систем из строя, в виду колоссального объема информации, обрабатываемой информационными системами правоохранительных органов; нехватка кадров, способных разрабатывать, грамотно и максимально результативно использовать информационные технологии¹.

Полагается, что направление развития информационных технологий в правоохранительной деятельности будет стремиться к решению данных проблем.

1.3 Правовое регулирование применения информационных технологий в правоохранительной деятельности

В юриспруденции под правовым регулированием понимают процесс целенаправленного воздействия государства, его органов и должностных лиц на общественные отношения при помощи юридических средств и методов, которые направлены на их стабилизацию и упорядочивание. При этом, под правовыми основами правоохранительной деятельности принято считать совокупность нормативных правовых актов, участником которых являются правоохранительные органы и их сотрудники. В данном случае законы и подзаконные нормативные акты должны устанавливать цели, задачи и принципы правоохранительного органа; их компетенцию, обязанности и права; гарантии соблюдения прав, свобод и законных интересов граждан; меры социальной и правовой защищенности должностных лиц. Это в полной мере можно отнести к правовой основе использования информационных технологий в правоохранительной деятельности.

Таким образом под правовым регулированием применения информационных технологий в правоохранительной деятельности мы можем

¹ Перед нами стоит задача провести в МВД техническую революцию: сайт МВД России. URL: http://www.mvd.ru/mvd/structure/unit/object/publications/show_8506

понимать систему правил и предписаний, содержащихся в законах и подзаконных нормативных правовых актах, которые устанавливают:

- цели, задачи и принципы использования информационных технологий в деятельности правоохранительных органов;
- компетенцию, права и обязанности каждого из органов, использующих информационные технологии для решения стоящих перед ними специальных задач;
- условия и правила их применения;
- гарантии соблюдения прав, свобод и законных интересов граждан;
- формы надзора и контроля в этой сфере.

В научной литературе систему нормативно-правовых источников, составляющих основу правоохранительной деятельности, принято делить на три уровня: федеральный, региональный и местный¹.

Федеральный уровень, безусловно, возглавляет Конституция РФ – первый подуровень федеральных актов, составляющих нормативно-правовую основу правоохранительной деятельности. Вторым подуровнем являются федеральные конституционные законы и федеральные законы. А также к ним относятся нормативные указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ, акты палат Федерального Собрания РФ, решения высших судебных инстанций РФ, акты Генеральной прокуратуры РФ и акты других федеральных органов государственной власти. Ведомственные нормативно-правовые акты представляют собой третий подуровень.

Региональный уровень также состоит из трех подуровней: конституции республик, уставы иных субъектов РФ; законы субъектов РФ, регулирующие отношения в данной сфере; подзаконные нормативно-правовые акты, принятые органами государственной власти данных субъектов.

¹ Пинчугина Е.Н. Правовая основа деятельности органов внутренних дел: понятие специфика, уровневая организация // Огарев-Online. – 2014. – №11 (25). – С. 4.

Местный (муниципальный) уровень образуют акты, принимаемые органами местного самоуправления. Это могут быть уставы муниципальных образований, акты выборных представительных и исполнительных органов местного самоуправления, а также должностных лиц этих органов и др.

В нормативно правовую основу правоохранительной деятельности включаются и международно-правовые акты, и принципы, которые являются частью национальной правовой системы России (п.4 ст.15 Конституции Российской Федерации).

Охарактеризуем основные акты, составляющие нормативно-правовую основу использования информационных технологий в правоохранительной деятельности. В первую очередь рассмотрим Конституцию Российской Федерации. Конституция Российской Федерации является основным законом государства и фундаментальным источником правового регулирования всего многообразия направлений правоохранительной деятельности. На ее основе разработаны принципы деятельности полиции, которые нашли свое нормативное правовое закрепление в гл. 2 ФЗ «О Полиции», ст. 3 ФЗ «Об Оперативно-розыскной деятельности», ст. 4 ФЗ «О прокуратуре Российской Федерации», ст. 5 ФЗ «О следственном комитете Российской Федерации» и т.д. Конституция Российской Федерации содержит основные предписания по вопросам обеспечения прав и свобод граждан (ст. ст. 20 – 44), охраны собственности (ст. 8). Важно отметить, что в тексте основного закона нашего государства содержится ряд норм, имеющих отношение к информационному обеспечению правоохранительных органов. Так, в статье 29 говорится, что «...каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»¹.

Кроме этого, ч.2 ст.23, ст. ст. 24, 25, ст.45 Конституции Российской Федерации в той или иной мере затрагивают вопросы получения информации, интересующей правоохранительные органы, в частности ОВД.

¹ Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года. // Российская газета. – 1993. – 25 декабря.

Так, нарушение прав и свобод граждан на неприкосновенность частной жизни, тайну переписки, неприкосновенность жилища и т.д. допускается лишь в случаях, предусмотренных федеральным законом и с разрешения суда. Деятельность ОВД по сбору такой информации должна преследовать цели борьбы с преступностью и только в рамках федерального законодательства.

Наряду с Конституцией Российской Федерации к первой группе нормативных актов, регулирующих правоохранительную деятельность по использованию информационных технологий, мы отнесем федеральные законы, в том числе кодифицированные. Проанализируем Уголовный кодекс Российской Федерации. Как мы знаем, оперативно-разыскная деятельность органов внутренних дел широко использует информационные технологии для решения поставленных перед ней задач.

Так, ст. 15 УК РФ дает определение понятия тяжести преступления, признаки которого, в соответствии со ст. 8 ФЗ «Об оперативно-розыскной деятельности», являются условием проведения ряда оперативно-розыскных мероприятий с использованием информационных технологий. В случае неправомерного использования информационных технологий сотрудником ОВД, Уголовный кодекс Российской Федерации предусматривает ответственность за такое деяние, например, ст. 137 «Нарушение неприкосновенности частной жизни», ст. 286 «Превышение должностных полномочий», ст. 272 «Неправомерный доступ к компьютерной информации»¹ и т.д.

Предпосылки для применения информационных технологий в правоохранительной деятельности также создает Уголовно-процессуальный кодекс Российской Федерации. Данный закон играет существенную роль в регулировании регистрационной деятельности ОВД в плане ведения криминалистических учетов. Соответствующие указания опосредованно

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ // СЗ РФ. – 1996. – №25. – Ст. 2954.

содержаться в ст. ст. 6, 9, 11, 21 УПК РФ. Также следует отметить, что использование информационных технологий в ОРД ОВД призвано способствовать успешному осуществлению процессуальной деятельности и, следовательно, реализации уголовного и уголовно-процессуального права. Это связано с тем, что, полученная законным путем, оперативно-розыскная и иная информация может служить поводом для возбуждения уголовного дела, быть использованной для подготовки и осуществления следственных и судебных действий, а также представлять в орган дознания, следствия или суд в качестве доказательств по уголовным делам, если они отвечают требованиям, предъявляемым к доказательствам установленным Уголовно-процессуальным кодексом Российской Федерации¹.

Следующим нормативным документом, затрагивающим вопросы применения информационных технологий в правоохранительной деятельности, является Федеральный закон «О полиции». Так, ст. 11 прямо указывает на обязанность полиции использовать в своей деятельности достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Закон дает право на использование электронной формы при приеме и регистрации документов, при уведомлении о ходе предоставления государственных услуг, а также при взаимодействии с органами государственной власти и общественными объединениями; право на применение технических средств при документировании обстоятельств совершения преступления и др.².

Таким образом положения Закона содержат точное указание на правомочие полиции использовать информационные технологии в различных направлениях своей деятельности. Данное положение подтверждается также Федеральным законом «Об оперативно-розыскной

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. №174-ФЗ // СЗ РФ. – 2001. – №52 (ч.1). – Ст. 4921.

² Федеральный закон «О полиции» от 7 февраля 2011 г. №3-ФЗ // СЗ РФ. – 2011. – №7. – Ст. 900

деятельности»¹. Согласно ст. 10 данного федерального закона, органы осуществляющие ОРД «в ходе проведения оперативно-розыскных мероприятий используют информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические средства и иные средства...».

Указы Президента Российской Федерации и нормативно-правовые акты Правительства Российской Федерации существенно не влияют на формирование правовой основы применения информационных технологий в правоохранительной деятельности.

Нормативные акты МВД России составляют большую часть всей системы нормативно-правовой основы организации и деятельности ОВД в целом. Их изучение показывает, что общие вопросы использования информационных технологий в деятельности ОВД не регулирует ни один нормативный правовой акт, хотя косвенно о них упоминается. Вполне вероятно, что конкретные вопросы использования информационных технологий в правоохранительной деятельности регламентируются внутриведомственными и межведомственными нормативными актами с грифом «ДСП».

Таким образом, анализ правовой основы использования информационных технологий в деятельности ОВД позволил выявить ряд недостатков в исследуемой сфере. Наиболее существенной проблемой в нормативной базе обеспечения применения информационных технологий в правоохранительной деятельности является ее полное отсутствие. Нормы в данной области раскиданы по нормативным актам различных уровней.

Так, Конституция РФ содержит принципы использования информационных технологий в правоохранительной деятельности; Уголовный кодекс РФ раскрывает некоторые основания их применения, а также формулирует ответственность при их незаконном использовании

¹ Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ // СЗ РФ. – 1995. – №33. – Ст. 3349

сотрудниками правоохранительных органов; нормы Уголовно-процессуального кодекса РФ применяются при оценке доказательств полученных с использованием информационных технологий, а также формулирует принципы уголовного судопроизводства; Федеральные Законы дают право на использование информационных технологий правоохранительными органами для решения поставленных перед ними задач; внутриведомственные нормативные акты не указывают на общие положения использования информационных технологий в своей деятельности.

Наблюдаются более конкретные пробелы правового регулирования отдельных аспектов в деятельности правоохранительных органов, связанных с информационными технологиями. Так, к примеру, несмотря на широкое применение электронного документооборота в деятельности граждан и организаций, УПК РФ не успевает отвечать всем вызовам, которые бросает ему развитие информационных технологий.

В то время как учёные и практики уже ввели в обиход такие термины, как «цифровая информация»¹, «электронные доказательства»², а некоторые исследователи даже говорят о необходимости введения электронных уголовных дел³, законодатель в этом плане остается консерватором.

Полагаем, данные положения выступают в качестве значительного упущения законодателя, поскольку закон должен соответствовать тенденциям развития современного общества, в том числе сфере информационных технологий. В противном случае закон перестанет работать

¹ Васюков В.Ф. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел // Известия ТулГУ. Экономические и юридические науки. – 2016. – № 3. – С. 203.

² Оконенко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. - 2015. – № 3 – С. 122.

³ Зуев С.В., Никтин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. – 2017. – № 3. – С. 590.

должным образом. Сейчас крайне важна более детальная регламентация информационных технологий в деятельности правоохранительных органов.

Подводя итоги нашего исследования в рамках первой главы, мы можем сделать следующие выводы.

Информационные технологии в правоохранительной деятельности начали свое развитие с момента появления первых ЭВМ в правоохранительных органах (1968 г.). Осознавая перспективность использования информационных технологий в практической деятельности правоохранительные органы пытаются использовать положительный опыт ИТ-отраслей.

Основными используемыми информационными технологиями в правоохранительной деятельности являются автоматизированные информационные технологии, представленные в виде автоматизированных информационных систем различных видов и автоматизированных рабочих мест.

Автоматизированные информационные технологии – система методов и способов сбора, накопления, хранения, поиска, обработки и защиты информации на основе применения развитого программного обеспечения, средств вычислительной техники и связи, а также способов, с помощью которых эта информация предоставляется пользователям.

В каждом правоохранительном органе используются данные информационные технологии, которые позволяют как обеспечить доступ гражданам к информации, так и использовать их для более эффективной работы, применяющиеся для сбора и обработки учетной и статистической информации, оперативной и следственной практики, криминалистические данные.

Среди действующих эффективных информационных технологий, обеспечивающих общественную безопасность, охрану прав и свобод граждан, следует назвать видеонаблюдение и видеофиксацию, в том числе снятие, обработку и передачу с камер видеонаблюдения видеопотока о

правонарушениях и ситуациях чрезвычайного характера, включая повреждения коммуникаций, инфраструктуры и имущества. В этом случае проводится анализ видео- и аудиопотоков, который предусматривает: автоматическую регистрацию событий на базе системы видеонализа потока, видеонализ событий, аналитику видеопотока в режиме реального времени, идентификацию и распознавание лиц.

Также, в правоохранительной деятельности информационные технологии предоставляют уникальную возможность определять местонахождение подвижных объектов. Примером геоинформационной системы может служить система «ГЛОНАСС», которая представляет собой интеграцию массивов обычной (фактографической) информации относительно объектов учета с массивами географической информации, представленной в виде топографических карт, планов и т.д. Использование таких систем в подразделениях МВД России позволяет получать наглядную информацию об определенных объектах в их пространственном расположении на картах или планах.

Правоохранительные органы при расследовании, раскрытии и пресечении правонарушений и преступлений используют различные информационные технологии, но единой методологии и правовой поддержки использования этих средств пока не существует. Содержатся только отдельные положения, упоминающие различные информационные технологии, однако данные положения фактически разбросаны по правовым актам различного уровня регулирования.

Тем не менее, современные информационные технологии позволяют выявить и своевременно пресечь правонарушение или готовящееся преступление в местах высокого риска террористической угрозы, изучить личности субъектов преступной деятельности, принять правильное решение в условиях тактического риска, оказать некоторые государственные услуги в электронной форме и т.д.

2 ПЕРСПЕКТИВЫ РАЗВИТИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

2.1 Информационное обеспечение раскрытия и расследования преступлений с помощью компьютерной техники

Понятие и сущность информационного обеспечения правоохранительной деятельности определяется характером и видом этой деятельности. В то время как информационное обеспечение деятельности по раскрытию и расследованию преступлений определяется деятельностью субъектов уголовного процесса (органы следствия и дознания, экспертно-криминалистические подразделения).

Следует отметить, что общей задачей информационного обеспечения раскрытия и расследования преступлений в целом является содействие борьбе с преступностью путем сбора, накопления, обработки и систематизации оперативно значимой информации.

Успешное расследование преступлений во многом зависит от объема информации, полученной сотрудником на первоначальном этапе расследования. Благодаря достаточному объему собранной информации сотрудник выбирает наиболее правильный путь расследования преступления. В связи с этим достигается целесообразность, экономичность использования сил и средств ОРД и деятельности следователя.

В настоящее время существует тенденция компьютеризации правоохранительной деятельности. Так, применяются различные компьютерные программы, раскрывающие алгоритмы раскрытия отдельных видов преступлений, а также используются программные средства «Автоматизированное рабочее место», технические средства цифровой фиксации аудио и видео информации и т.д.

В рамках данного параграфа рассмотрим подробнее программный комплекс АРМ на примере профессиональной деятельности следователя. Автоматизированное рабочее место следователя («АРМ следователя») - это комплекс технических и программных средств для работы с различными базами данных при расследовании преступлений. Другими словами программное обеспечение «АРМ следователь» предназначено для информационного обеспечения деятельности следователя, путем автоматизации его деятельности. Программный комплекс выполняет ряд задач, однако основная заключается в накоплении следственной информации путем организации единого учета. Также он способствует самоорганизации следователя за счет предоставления информации о сроках предварительного следствия и хода расследования.

Тем не менее, следует отметить, что в ходе расследования следователь, как и раньше, полагается на свои профессиональные знания и умения, приобретенные его практическим опытом. Однако в криминалистике существует четкая алгоритмизация процессов дознания и предварительного следствия. Разработаны алгоритмы расследования конкретных видов преступления, которые включают в себя как общий процесс расследования, так и проведения отдельных следственных действий.

М.Б. Вандер отмечает: «криминалистический алгоритм – это система установленных законом и установленных криминалистикой предписаний, выполнение которых направлено на эффективное решение задач по расследованию, раскрытию и предупреждению преступлений. Криминалистический алгоритм не является строго обязательным, ему свойственен также эмпирический характер, что обеспечивает свободу мысли следователя в принятии им на любой стадии расследования решения о проведении тех или иных процессуальных действий»¹.

¹ Вандер М.Б. Проблемы формирования инновационной технологии расследования преступлений // КриминалистЪ – 2008. – №2. – С. 40

Необходимо подчеркнуть, что успех выявления и раскрытия преступления зависит не столько от правильного усвоения методологических рекомендаций, сколько от их грамотного применения. Таким образом методологические предписания выступают лишь предпосылкой деятельности сотрудников дознания и следствия.

Для того, чтобы использование методик раскрытия отдельных видов преступления было наиболее эффективным, должны соблюдаться определенные требования в ее разработке.

Опираясь на теоретические положения ученых-криминалистов¹ по проблемам программирования расследования можно выделить следующие требования, которым должны отвечать разрабатываемые программы:

– Рекомендательный характер. Программа должна представлять собой систему рекомендаций, советов, рассчитанных лишь на определенный этап расследования, а не систему команд и предписаний, подавляющих инициативу следователя, дознавателя. То есть за сотрудником должно оставаться право самому принимать решение и иметь творческий подход в расследовании.

– Научность и законность. Программа должна базироваться на научных данных, изучении специальной литературы, материалах обобщения оперативно-розыскной и следственной практики и, конечно же, соответствовать действующему законодательству.

– Оптимальность. Программа должна быть компактной и точной, но в то же время описание должно быть емким, позволяющим видеть описываемый объект, во всем его многообразии и сложности. Рекомендации, содержащиеся в программе, должны быть простыми, краткими, ясными, определенными и практически выполнимыми.

¹ Шаталов А.С. проблемы алгоритмизации расследования преступлений: Дис. ... д-ра юрид. наук. – М., 2000; Сливинский К.О. Алгоритмизация деятельности следователя. Дис. ... канд. юрид. наук. – М., 2004.

– Указывать не вероятностный характер типичных версий. Необходимо, чтобы работник обрабатывал все возможные версии, а не только те, что выдала программа. В случае нетипичной следственной ситуации, расследовать и раскрыть ее с помощью типовой программы будет невозможно.

– Гибкость и многовариантность. Данное требование обусловлено тем, что каждое преступление различается между собой, даже если совершен один и то же преступление по уголовному кодексу. Создание эффективной программы раскрытия преступлений обеспечивается применением метода обобщения ситуации, суть которого заключается в том, что несколько конкретных преступлений одного вида, объединяются в одну или несколько обобщенных ситуаций, для которых и разрабатывается оптимальная программа принятия решений и проведения следственных действий.

– Эффективность и результативность. Программа должна быть направлена на облегчение деятельности по расследованию и раскрытию преступлений, экономить время, силы и средства сотрудников.

Большинство рекомендаций по применению методик расследования отдельных видов преступления носят печатный характер, представляя собой учебные пособия, методические рекомендации.

Невозможно не согласиться с мнением Р.С. Белкина, что неопытный следователь в экстремальной ситуации или в условиях дефицита времени не сможет вспомнить десятки страниц «книжной методики» первоначального этапа расследования определенного вида преступления или конкретного следственного действия¹. Это представляет собой проблему для оперативного, целенаправленного и верного принятия необходимых действий, а, следовательно, ухудшает качество проводимого расследования и неоправданно увеличивает срок расследования преступления.

¹ Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы современной криминалистики.– М., 2001. – С. 127.

По мнению И.Н. Пустовой решением данной проблемы послужит создание научных рекомендаций, позволяющих следователю и дознавателю в кратчайшие сроки совершать последовательные операции по конкретной, заранее разработанной схеме, представленной в виде криминалистических алгоритмов или программ расследования¹. Действительно, их применение поможет дознавателю, следователю сконцентрировать внимание на всех необходимых направлениях деятельности по расследованию преступлений и, что самое важное, окажет реальную интеллектуальную поддержку в решении задач в максимально короткие сроки.

В настоящее время разрабатываются информационные технологии, направленные на упрощение работы следователя. Речь идет о компьютерных программах по раскрытию и расследованию преступлений.

Исследование литературы показало, что ученые давно рассматривают вопросы разработки компьютерных программ по расследованию и раскрытию преступлений². Однако теоретические разработки очень медленно реализуются в практическую деятельность. Программирование раскрытия и расследования преступлений, с применением современных информационных технологий являются на современном этапе первоочередными задачами.

По нашему мнению, опыт ученых позволит создать информационную технологию, в которой возможности компьютерной техники и программных средств будут сопровождать следователя на всех этапах расследования преступления вплоть до составления решения по уголовному делу. Это является актуальной задачей сегодняшнего дня и, следует заметить, что она уже реализуется. Так, на базе Нижегородского государственного

¹ Пустовая И.Н. Вопросы разработки компьютерных программ расследования преступлений. // Правопорядок: история, теория, практика. – 2018. – №4. – С. 27

² Дробатухин В.С. Кибернетическое моделирование при расследовании преступлений / В.С. Дробатухин: автореф. дисс. ... канд. юрид. наук. – М., 1998; Куриленко Ю.А. Компьютерные технологии как средство повышения эффективности организации правоохранительной деятельности (приминительно к деятельности ОВД по расследованию преступлений) / Ю.А. Куриленко: автореф. ... канд. юрид. наук. – Саратов, 2008.

университета имени Н.И. Лобачевского, под руководством профессора В.Ю. Толстолицкого была создана программа, сочетающая в себе автоматизированные информационно-логические системы (АИЛС) и широко применяемые автоматизированные информационно-поисковые системы (АИПС). Представителем данной системы является компьютерная криминалистическая программа «ФОРВЕР», способная формулировать версии и содержащая в себе технологию раскрытия преступлений¹.

Расследование преступлений представляет собой особую разновидность интеллектуальной деятельности. Наиболее сложными ее элементами являются анализ и оценка сложившейся следственной ситуации, которые предшествуют совершению всех процессуальных действий. Все это сопровождается трудоемкой, монотонной, сугубо технической работой следователя.

Для успешного решения стоящих перед ним задач в криминалистике объективно существует унифицированная система научных положений и основанных на них рекомендаций, представленная для практического использования в виде криминалистических алгоритмов и программ расследования. Программирование правоохранительной деятельности позволяет сотрудникам ускорить процесс и повысить качество расследования уголовных дел.

2.2 Использование сети Интернет для решения задач по раскрытию преступлений

Глобальная сеть Интернет в правоохранительной деятельности, по мнению Жукова А.И., представляет собой современную информационную площадку, ставшей полноценным средством массовой информации и

¹ Толстолицкий В.Ю. Использование информационных технологий в раскрытии и расследовании убийств: электронное учебно-методическое пособие. – Нижний Новгород: Нижегородский государственный университет. – 2012. – С. 83.

используемой государственными органами, уполномоченными осуществлять деятельность по охране правопорядка и законности, защите прав и свобод человека, с целью раскрытия, расследования, пресечения преступлений, получения необходимой информации¹.

Современное общество использует Интернет практически во всех сферах жизни. Данное явление дает начало как позитивным, так и негативным последствиям, таким как появление новых способов совершения преступлений. Особую опасность Интернет представляет потому, что он является огромным рынком нелегальной продукции; им активно пользуются преступники при общении между собой, а также при поиске жертвы, через Интернет совершаются ряд краж, мошенничества, террористическая экстремистская деятельность, пропаганда антисоциального образа жизни, что в целом может представлять угрозу национальной безопасности.

Одним из условий успешного расследования и раскрытия преступлений, совершаемых с использованием сети Интернет, является постоянное совершенствование теоретических и практических знаний сотрудников, осуществляющих правоохранительную деятельность, а также применение современных информационных технологий в своей деятельности, поиск новых способов сбора доказательств по делу.

Как нами было указано в первой главе, информация – это необходимый элемент в расследовании преступлений. Поиск информации, ее фиксация и анализ занимают центральное место в деятельности органов дознания и следствия. Хорошие возможности работы с информацией предоставляет Интернет, в особенности социальные сети.

Важной особенностью сети Интернет является то, что информация в социальных сетях имеет свойство храниться долгий промежуток времени. Все, что пользователь выкладывал в своем аккаунте: личная информация,

¹ Жуков А.И. Современные проблемы использования Интернета в расследовании и раскрытии преступлений. // Проблемы современной науки и образования. – 2017. – №25. – С. 44.

фотографии, видео, комментарии, записи, все личные переписки, все это хранится на сервере и будет храниться долгое время, даже если пользователь удалит эту информацию. При этом, если человек не регистрировался ни в каких социальных сетях, информация о нем может быть обнаружена на страницах других пользователей, например в случае выкладывания общей фотографии его знакомым.

В Самарском национальном исследовательском университете имени академика С.П. Королёва в течение 2015-2016 учебного года в рамках дисциплины «Криминалистика» среди студентов проводился эксперимент по сравнению и сопоставлению различных способов сбора информации о личности: с помощью сети Интернет и традиционного опроса. Результаты исследования показали целесообразность и преимущество использования сети Интернет для поиска сведений об интересующей личности, поскольку мониторинг социальных сетей позволил получить значительное количество информации за сравнительно короткий период. В среднем за 2,5 часа удавалось составить достаточно подробное досье человеку без использования специальных знаний и программных продуктов¹.

Таким образом, для поиска, получения и обработки большого количества информации в сети Интернет не обязательно наличие специальных знаний и программных продуктов, а достаточно умения пользоваться поисковыми системами (например, google), социальными сетями (например, ВКонтакте, Одноклассники, Твиттер и др.), специальными сайтами (например, «Юла», «налог.ру»). Такие инструменты смогут помочь в работе правоохранительных органов, существенно сократив время на поиск информации и обеспечив некоторую самостоятельность сотрудников в связи с отсутствием необходимости привлекать дополнительных специалистов.

¹ Олиндер Н.В., Гамбарова Е.А. Проблемные вопросы поиска и восприятия информации о человеке в сети Интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. – 2016. – №4. – С. 55-60.

В качестве яркого примера использования интернет ресурсов в следственной практике можно привести уголовное дело по обвинению гр-на Коробова Е.В. в совершении преступления, предусмотренного ч. 1 ст.158 УК РФ. Данный пример отражает то, как использование сети Интернет позволяло раскрыть преступление по горячим следам - обнаружить и изъять похищенное имущество на следующий день после совершения преступления. Так, гр-н Коробов Е.В., тайно похитил два велосипеда и продал через сайт в Интернете по заниженной цене. Проведенный в интернете анализ сайтов, специализирующихся на продаже бытовой техники, позволил обнаружить объявление о продаже велосипеда, схожего по описанию с похищенным. Проведенной проверкой данный факт был подтвержден, имущество было изъято и возвращено законному владельцу¹.

В вышеприведенном примере использование сети Интернет в преступных целях использовалось только для сбыта похищенного имущества. Однако на практике существуют ситуации, когда преступление совершается непосредственно в интернете, от приготовления к преступлению до юридически законченного состава преступления. Например, создание сайта экстремистской направленности.

В таких случаях основной проблемой выявления, пресечения и раскрытия преступления является установление лица его совершившего. Причина кроется в том, что среда Интернет позволяет лицу совершать преступление, оставаясь неустановленным. Существуют программы, например Steganos Internet Privacy, которые уничтожают все следы пребывания лица, как в компьютере, так и в Интернете. Одновременно с этим данная программа позволяет скрыть пребывание в Интернете путем использования целой серии IP адресов, вместо реального IP адреса.

Конечно, несмотря на ряд трудностей, задача по пресечению преступлений, совершаемых в Интернет пространстве, остается. Один из

¹ Уголовное дело № 10-624/2018 из архива Тракторозаводского районного суда г. Челябинска.

вариантов ее реализации – использование систем блокирования информации, распространение которой представляет общественную опасность. Такие системы относятся к информационным технологиям.

Для решения данной задачи представляется необходимым разработать системы автоматизации поиска информации, имеющей антисоциальную направленность в сети Интернет и ее блокирование в автоматическом режиме с использованием информационных технологий.

Что касается непосредственного проведения ОРД для получения информации о разыскиваемых лицах с помощью сети Интернет, то нами представляется необходимым обозначить виды ОРМ, используемые в данных целях. Так, для получения компьютерной информации посредством проведения ОРМ в сети Интернет оперативными сотрудниками используются «Наведение справок», «Наблюдение», «Обследование помещений, зданий, сооружений, участков местности и транспортных средств», «Снятие информации с технических каналов связи».

6 июля 2016 г. перечень ОРМ был дополнен оперативно-розыскным мероприятием «Получение компьютерной информации»¹. По мнению С. В. Баженова, целью анализируемого ОРМ должно быть получение информации, для доступа к которой необходима помощь специалиста (преодоление технических или программных средств защиты, получение метаданных, пр.), а также использование специальной техники и (или) специальных программ оперативно-техническими подразделениями². Данное ОРМ осуществляется только негласно, что вытекает из анализа ч. 4 ст. 6 Закона об ОРД, где оговорено, что ряд оперативно-розыскных мероприятий, в том числе связанных с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов Федеральной

¹ Федеральный Закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ // СЗ РФ. – 1995. – №33. – Ст. 3349.

² Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. – 2017. – № 2(65). – С.32.

службы безопасности, органов внутренних дел в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность, тем самым определен специальный субъект проведения и негласный характер этого ОРМ. Но до настоящего времени на ведомственном уровне нет никаких разъяснений по этому поводу, отсутствует и соответствующий нормативный акт¹. Таким образом, сотрудники розыскных подразделений понимают, что сведения о разыскиваемых лицах можно получать посредством технических средств через Интернет, но не всегда верно определяют инструментарий получения необходимых сведений, интуитивно избирая оперативно-розыскные мероприятия «Наведение справок», «Наблюдение», «Обследование», «СИТКС».

Подводя итоги, мы можем сделать вывод, что социальные сети - важный источник информации, который может быть использован следователем в своей работе. Социальные сети как инструмент в расследовании удобны своей доступностью (не требуют профессиональных познаний в компьютерной технике), скоростью извлечения и объемом информации, которая может быть получена.

В настоящее время представляется целесообразным и важным разработать методические рекомендации для сотрудников правоохранительных органов, устанавливающих механизм поиска информации в сети Интернет. Построение алгоритма решения профессиональной задачи, включающего в себя: выделение этапов процесса обработки данных; формальное определение их содержания и порядка их выполнения; разработка шаблона действий и/или мыслительных операций, позволяет оптимизировать поисково-познавательную, организационно-технологическую составляющую активного взаимодействия лица, ведущего расследование, с объектами окружающего мира, связанными с преступным событием.

¹ Там же. С. 33.

2.3 Совершенствование информационных технологий в правоохранительной деятельности

По нашему мнению, исследование в данном направлении должно осуществляться в трех направлениях:

1. анализ законодательной базы и выявление проблем в правовом регулировании использования информационных технологий в правоохранительной деятельности;
2. изучение современного состояния информационных технологий в правоохранительной деятельности с точки зрения полноты решения задач, стоящих перед правоохранительными органами, а также соответствия тенденциям развития Российской Федерации в рамках национальной программы «Цифровая экономика», в целях решения практических проблем их применения;
3. рассмотрение зарубежного опыта, как основы совершенствования правоохранительной деятельности в области использования информационных технологий.

Структура нашей работы была составлена таким образом, что первые два пункта направления исследования, о которых говорится выше были изучены и проанализированы ранее. В данном параграфе нам остается только обозначить проблемы и предложить пути их решения. А также рассмотреть зарубежный опыт.

Мировой тенденцией является переход к информационному обществу, повсеместное внедрение информационных технологий и реализация государственных программ цифрового развития. Опыт передовых в области цифровизации стран, таких, как Сингапур, Норвегия, США, показывает, что главенствующая роль в вопросах формирования национальной стратегии

информационного развития отводится государству¹. Аналогичная ситуация складывается в странах постсоветского пространства, в связи с чем мы рассмотрим государственный подход к цифровизации правоохранительной деятельности в Казахстане.

Так, в рамках госпрограммы «Цифровой Казахстан» предусмотрена реализация трех информационных проектов МВД:

1. Информационная система «База данных участковых-уполномоченных полиции». Обеспечить каждому УУП доступ к централизованным базам данных МВД, путем использования персонального планшетного компьютера независимо от времени и места его нахождения. Данная система дает возможность при несении службы УУП оперативно проверять гражданина по учетам в БД МВД и на месте в электронном виде составлять необходимые процессуальные документы. К тому же в систему будут своевременно вводиться изменения, касающиеся административного участка. Предполагается также создание так называемой «интернет площадки» посредством которого граждане смогут в онлайн режиме обращаться к участковому инспектору, отслеживать статус своего обращения, получать сведения о состоянии дел в районе проживания, сообщать об известных фактах правонарушения и вносить предложения.

2. Автоматизированная информационная система «Следователь». Предполагается оснастить всех следователей и дознавателей именными планшетами, которые позволят заметно ускорить процесс и повысить качество расследования уголовных дел. У следователя появится возможность моментального доступа ко всем информационным ресурсам госорганов. При этом сотрудники, находясь на месте происшествия, смогут получать в электронном виде методические рекомендации по выбору тактики и метода расследования конкретного преступления. При проведении осмотров места

¹ Тишкова И.В. Сравнительный анализ использования информационно-коммуникационных технологий в России и зарубежных странах // Современный ученый. – 2017. – № 2. – С. 132.

происшествия, допросы и другие система способна в автоматизированном режиме обеспечивать следователя, дознавателя формализованными бланками процессуальных документов.

3. Центры оперативного управления малых городов республики Казахстан. Главная задача – оперативное реагирование на любое правонарушение на улицах или других общественных местах, а также автоматизация всего процесса и обеспечение контроля на всех стадиях.

МВД республики Казахстан разработал хорошую базу информационных систем в правоохранительной деятельности, отвечающей современным потребностям в формировании цифрового общества, а также способную повысить качество и скорость работы сотрудников полиции, оперативно решать задачи, стоящие перед сотрудниками МВД.

Анализ правовой основы использования информационных технологий в правоохранительной деятельности позволил выявить ряд недостатков в исследуемой сфере. Наиболее существенной проблемой в нормативной базе обеспечения применения информационных технологий в правоохранительной деятельности является ее полное отсутствие. Нормы в данной области раскиданы по нормативным актам различных уровней.

Наблюдаются более конкретные пробелы правового регулирования отдельных аспектов в деятельности правоохранительных органов, связанных с информационными технологиями. Так, к примеру, несмотря на широкое применение электронного документооборота в деятельности граждан и организаций, УПК РФ не успевает отвечать всем вызовам, которые бросает ему развитие информационных технологий.

При изучении современного состояния информационных систем для решения задач правоохранительной деятельности нами была выделена такая проблема, как усложнение и совершенствование программного обеспечения. Дело в том, что возможности работы тех или иных программ постоянно расширяются, происходит обновление систем, но имеющееся оборудование

порой не в силах справляться с передачей данных этими программами, так как не обновляется столь же часто.

Так, в нашем анкетировании 70% дознавателей отмечали, что у них хотя бы раз, но возникали трудности в использовании информационных систем. Среди основных трудностей сотрудники отметили следующее: сбои в системах и подключениях, частая смена паролей и логинов для доступа к информационным системам, иные проблемы технического характера, а также нехватка специальных знаний.

Еще одной проблемой в применении информационных систем в правоохранительной деятельности на сегодняшний день является обеспечение безопасности информационных правоохранительных систем. Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры¹.

Проблема информационной безопасности для правоохранительных органов на сегодняшний день представляет наибольший интерес. Она носит комплексный характер, для решения которой необходимо сочетание законодательных, организационных и программно-технических мер.

Наблюдается огромная нехватка высококвалифицированных кадров по внедрениям информационных технологий, а также по обеспечению информационной безопасности.

Рассматривая комплекс вышеназванных проблем, мы считаем, что для их решения необходимо:

1. разработать единые правовые методические, программные, технические подходы для организации единой системы информационного обеспечения каждого государственного и правоохранительного органа;

¹ Галатенко В. Информационная безопасность: Открытые системы, 1996. – № 1. – С 38.

2. создать единые системы пользования банков данных коллективного пользования криминалистической, оперативно-справочной, розыскной и прочей информации, при которой у каждого государственного органа будет возможность использовать банки данных другого органа, и при этом осуществлять деятельность по направлению запросов и пр.;

3. обеспечить планомерный переход на безбумажные технологии сбора, обработки, хранения и передачи информации;

4. обеспечить совершенствование правового, организационного и технического обеспечения мероприятий, направленных на укрепление режима защиты конфиденциальной информации и персональных данных;

5. продолжить тенденцию информатизации и автоматизации ведения расследования дел.

Процесс внедрения информационных технологий в правоохранительных органах не обходится без ряда проблем. Во-первых, это отсутствие нормативной базы регулирования применения информационных технологий в правоохранительной деятельности, методических, программных, технических подходов для организации единой системы информационного обеспечения каждого государственного и правоохранительного органа. Во-вторых, в связи с внедрением и развитием информационных систем, особое значение имеет информационная безопасность. В-третьих, это отсутствие у специалистов специальных знаний по использованию информационных технологий, что приводит к тому, что информационные технологии, направленные на мобильность работы с информацией, требуют опытного внедрения, в процессе которого чаще всего происходят сбои в работе. При решении проблем информатизации правоохранительных органов за основу должен браться передовой международный опыт.

ЗАКЛЮЧЕНИЕ

Данные международных рейтингов по цифровизации государств показали наше недостаточное совершенство в этой области. Решая проблемы внедрения информационных технологий, следует опираться на международный опыт в этой сфере и переходить на максимально полную цифровизацию предоставления государственных услуг, электронные дела, электронное общение между органами через единые информационные системы.

Состояние обеспечения правоохранительной деятельности информационными технологиями в последнее время находится на достаточно качественном организационном уровне, что показывает практика их применения, исследованная в данной работе. Однако, несмотря на определенные успехи, ощущается несовершенство правового и организационного обеспечения развития информационных технологий в правоохранительной деятельности.

Анализ современного этапа использования информационных технологий в правоохранительной деятельности показал отсутствие единых информационных систем, через которые государственные органы могли бы взаимодействовать друг с другом напрямую и оперативно. К тому же до сих пор в России наблюдается высокий уровень бюрократии, который проецируется, в том числе, и на применение информационных технологий правоохранительными органами. На наш взгляд, должны быть разработаны концепции информационных систем, которые смогли бы обеспечить взаимодействие государственных органов на более высоком уровне.

При изучении современного состояния информационных систем для решения задач правоохранительной деятельности нами была выделена такая проблема, как усложнение и совершенствование программного обеспечения. Дело в том, что возможности работы тех или иных программ постоянно расширяются, происходит обновление систем, но имеющееся оборудование

порой не в силах справляться с передачей данных этими программами, так как не обновляется столь же часто.

Еще одной проблемой в применении информационных систем в правоохранительной деятельности на сегодняшний день является обеспечение безопасности информационных правоохранительных систем. Проблема информационной безопасности для правоохранительных органов на сегодняшний день представляет наибольший интерес. Она носит комплексный характер, для решения которой необходимо сочетание законодательных, организационных и программно-технических мер.

Усматривая огромная нехватка высококвалифицированных кадров по внедрениям информационных технологий, а также по обеспечению информационной безопасности в правоохранительных органах, что тоже является немаловажным аспектом в достижении целей по информатизации правоохранительной деятельности.

Информатизация системы правоохранительных органов в Российской Федерации – незаменимый и важный этап в становлении системы, а также ведущее направление реформирования. Поэтому, рассматривая комплекс проблем, нами в данной работе предложены следующие решения:

- необходимо разработать единые правовые методические, программные, технические подходы для организации единой системы информационного обеспечения каждого государственного и правоохранительного органа;

- создать единые системы пользования банков данных коллективного пользования криминалистической, оперативно-справочной, розыскной и прочей информации, при которой у каждого государственного органа будет возможность использовать банки данных другого органа, и при этом осуществлять деятельность по направлению запросов и пр.;

- обеспечить планомерный переход на безбумажные технологии сбора, обработки, хранения и передачи информации;

– обеспечить совершенствование правового, организационного и технического обеспечения мероприятий, направленных на укрепление режима защиты конфиденциальной информации и персональных данных;

– представляется возможным постановка вопроса о совершенствовании процесса подготовки сотрудников правоохранительных органов и судов, специализирующихся на работе в области информационных технологий и информационной безопасности.

Проблемы применения информационных технологий в правоохранительной и правоприменительной деятельности вполне разрешимы, но требуют постоянного мониторинга, а также технического, организационного и законодательного усовершенствования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Раздел 1 Нормативные правовые акты и иные официальные акты

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года. // Российская газета. – 1993. – 25 декабря.
2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. №174-ФЗ // Собрание законодательства РФ. – 2001. – №52 (ч.1). – Ст. 4921.
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ // Собрание законодательства РФ. – 1996. – №25. – Ст. 2954.
4. Федеральный закон «О полиции» от 7 февраля 2011 г. №3-ФЗ // Собрание законодательства РФ. – 2011. – №7. – Ст. 900
5. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006г. №149-ФЗ // Собрание Законодательства РФ. – 2006. – №31 (1ч.). – Ст. 3448.
6. Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.
7. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ // Собрание законодательства РФ. – 1995. – №33. – Ст. 3349.
8. Закон РФ «О милиции» от 18.04.1991 № 1026-1 // Ведомости СНД и ВС РСФСР. – 1991. – №16. – Ст. 503.
9. Указ Президента Российской Федерации «Доктрина информационной безопасности» от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.
10. Распоряжение Правительства РФ «Об утверждении плана мероприятий («дорожной карты») по созданию открытого акционерного общества «ГЛОНАСС», развитию государственной автоматизированной

информационной системы «ЭРА-ГЛОНАСС» и ее использованию в интересах других информационно-навигационных комплексов и систем, создаваемых федеральными органами исполнительной власти и организациями» от 9 августа 2014 г. № 1498-р // Собрание законодательства РФ. – 2014. – №34. – Ст. 4693.

11. Приказ Генерального прокурора Российской Федерации «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» от 14.09.2017 № 627 // "Законность". - 2017. - №12. (Приказ)
12. Приказ МВД России "О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции" от 5 февраля 2016 г. №60. Документ официально опубликован не был. СПС «Консультант Плюс»
13. Приказ МВД России «Об организации научного обеспечения и применении положительного опыта в органах внутренних дел Российской Федерации и внутренних войсках МВД России» от 18 марта 2013 г. №150. Документ официально опубликован не был. СПС «Консультант Плюс»
14. Приказ МВД России «Об утверждении Концепции развития информационно-вычислительной системы МВД России на 2002-2006 годы» от 13 июня 2002 г. № 562. Документ официально опубликован не был. СПС «Консультант Плюс»

Раздел 2 Литература

15. Андреев, Н.Д. Современные системы информационного обеспечения сотрудников ОВД: монография / Н.Д. Андреев, В.В. Антонов. – Уфа: УЮИ МВД России, 2009. – 160 с.
16. Артамонова, Б.Н. Основы современных компьютерных технологий. / под ред. Б.Н. Артамонова. – СПб: КОРОНА принт, 2002. – 446 с.

17. Баженов, С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» / С.В. Баженов // Научный вестник Омской академии МВД России. – 2017. – № 2(65). – С. 31 – 34.
18. Белкин, Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы современной криминалистики. / Р.С. Белкин – М.: Норма, 2010. – 240 с.
19. Вандер, М.Б. Проблемы формирования инновационной технологии расследования преступлений / М.Б. Вандер // КриминалистЪ – 2008. – №2. – С. 40 – 43.
20. Васюков, В.Ф. Некоторые проблемы получения и использования цифровой информации при расследовании уголовных дел / В.Ф. Васюков // Известия ТулГУ. Экономические и юридические науки. – 2016. – № 3. – С. 201 – 205.
21. Грицаев, С.И. Особенности построения версий о лице, совершившем неочевидное преступление. / С.И. Грицаев, В.В. Помазанов // Евразийский юридический журнал. – 2018. – №8 (123). – С. 290 – 292.
22. Грицаев, С.И. Автоматизированное рабочее место следователя при производстве расследования: возможности и применение. / С.И. Грицаев, В.В. Помазанов // Российский следователь. – 2019. – №2. – С. 10 – 13.
23. Демидов, Л.Н. Информационные технологии. / под ред. Л.Н. Демидова – М.: КНОРУС, 2017. – 222 с.
24. Жуков, А.И. Современные проблемы использования Интернета в расследовании и раскрытии преступлений. / А.И. Жуков // Проблемы современной науки и образования. – 2017. – №25. – С. 43 – 46.
25. Зуев, С.В. Информационные технологии в решении уголовно-процессуальных проблем / С.В. Зуев, Е.В. Никитин // Всероссийский криминологический журнал. – 2017. – № 3. – С. 587 – 595.
26. Ивлев, А.Ф. Информационные технологии в организации прокурорского надзора / А.Ф. Ивлев, И.И. Потапова, Э.А. Сугаипова,

- Ю.А. Елисеева // Вестник Российской академии естественных наук. – 2015. – №19. – С. 7 – 12.
27. Коноплева, И.Л. Информационные технологии: Уч. пособие / под. ред. И.Л. Коноплевой. – М.: Право, 2009. – 294 с.
28. Лисенкова, Л.В. Влияние информационных технологий на прокуратуру / Л.В. Лисенко // Электронный вестник Ростовского социально-экономического института. – 2017. – №2. – С.138 – 143.
29. Оконенко, Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – №3 – С. 121 – 125.
30. Олиндер, Н.В. Проблемные вопросы поиска и восприятия информации о человеке в сети Интернет и ее использование при расследовании преступлений / Н.В. Олиндер, Е.А. Гамбарова // Юридический вестник Самарского университета. – 2016. – №4. – С. 55 – 60.
31. Паламарчук, С.А. Совершенствование конституционно-правового регулирования права на информацию в сети интернет / С.А. Паламарчук // Северокавказский юридический вестник. – 2015. – №4. – С. 108 – 114.
32. Пинчугина, Е.Н. Правовая основа деятельности органов внутренних дел: понятие специфика, уровневая организация / Е.Н. Пинчугина // Огарев-Online. – 2014. – №11 (25). – С. 1–7.
33. Пустовая, И.Н. Вопросы разработки компьютерных программ расследования преступлений. / И.Н. Пустовая // Правопорядок: история, теория, практика. – 2018. – №4. – С. 26 – 29.
34. Сливинский, К.О. Алгоритмизация деятельности следователя: дис. ... канд. юрид. наук. / К.О. Сливинский. – М., 2004. – 214 с.
35. Смахтин, Е.В. Некоторые вопросы использования систем видеонаблюдения в деятельности правоохранительных органов по раскрытию и расследованию преступлений. / Е.В. Смахтин, С.В.

Щербич // Российское право: Образование. Практика. Наука. – 2017. – №6 (102). – С. 77 – 82.

36. Тишкова И.В. Сравнительный анализ использования информационно коммуникационных технологий в России и зарубежных странах / И.В. Тишкова // Современный ученый. – 2017. – № 2. – С. 130 – 138.
37. Толстолицкий, В.Ю. Использование информационных технологий в раскрытии и расследовании убийств: электронное учебно-методическое пособие. / В.Ю.Толстолицкий. – Нижний Новгород: Нижегородский государственный университет. – 2012. – 150 с.
38. Цимбал, В.Н. Некоторые вопросы использования сотрудниками полиции информационных технологий / В.Н. Цимбал // Общество и право. – 2015. – №1 (51). – С. 232–235.
39. Шаталов, А.С. проблемы алгоритмизации расследования преступлений: дис. ... д-ра юрид. наук. / А.С. Шаталов. – М., 2000. – 411 с.

Раздел 3 Постановления высших судебных инстанций и материалы судебной практики

40. Уголовное дело № 10-624/2018 по обвинению Коробова Е.В. по ч.1 ст. 158 УК РФ / Архив Тракторозаводского районного суда г. Челябинска.
41. Приговор Калининского районного суда г. Челябинска № 1-648/2016 от 25 октября 2016 г. по делу № 1-648/2016 [Электронный ресурс]: Судебные и нормативные акты РФ. – URL: <http://sudact.ru> (дата обращения 05.06.2019 г.)

Раздел 4 Интернет источники

42. Официальный сайт Правительства РФ [Электронный ресурс] – Режим доступа: www.government.ru (дата обращения 13. 01. 2019).

43. Информационные технологии в МВД России // [Электронный ресурс] URL: <http://www.tadviser.ru/index.php/> (дата обращения 13.01.2019)
44. Образован Департамент информационных технологий, связи и защиты информации МВД России. // [Электронный ресурс] URL: <https://мвд.пф/news/item/172419> (дата обращения 13.01.2019)
45. Паспорт проекта цифровой трансформации органов и организаций прокуратуры Российской Федерации // [Электронный ресурс] URL: http://d-russia.ru/wp-content/uploads/2018/02/GP_trasnformatsia_plan.pdf. (дата обращения 03.03.2019)
46. Перед нами стоит задача провести в МВД техническую революцию. // [Электронный ресурс] URL: <http://www.mvd.ru/mvd/structure/unit/object> (дата обращения 28.01.2019)
47. Пресс-служба ГИАЦ МВД России [Электронный ресурс] – Режим доступа: <http://www.mvd/tu/news/31439> (дата обращения 03.03.2019)
48. Системы Папилон: официальный сайт [Электронный ресурс] – Режим доступа: www.papillon.ru (дата обращения 23.02.2019)
49. IMD World Competitiveness Center [Электронный ресурс] – Режим доступа: www.imd.org (дата обращения 02. 03. 2019)
50. International Telecommunication Union [Электронный ресурс] – Режим доступа: www.itu.int (дата обращения 02. 03. 2019)

**АНКЕТИРОВАНИЕ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ
ОРГАНОВ**

Кафедра правоохранительной деятельности и национальной безопасности Юридического института Южно-уральского государственного университета проводит социологическое исследование на тему «Информационные технологии как средство повышения эффективности организации правоохранительной деятельности» с целью выявления проблем обеспечения информационными технологиями правоохранительных органов.

Просим Вас принять участие в опросе и ответить на следующие вопросы:

1. Ваш возраст:

- до 25 лет
- 26-30
- 31-40
- 41 и старше

2. Какого уровня правоохранительный орган, в котором Вы работаете?

- федеральный;
- региональный;
- районный;
- городской;

Другое _____

3. Сотрудником какого правоохранительного органа Вы являетесь?

- системы МВД РФ;
- Прокуратура РФ;
- СК РФ;
- ФСБ;

Другое _____

4. Какую должность Вы занимаете?

5. Имеете ли Вы доступ к информационным технологиям (Автоматизированные рабочие места / Информационные системы / Технические средства)?

- да;
- нет;

Другое _____

6. Как часто вы используете их в процессе своей профессиональной деятельности?

- всегда;
- часто;
- редко.
- не использую совсем;
- Другое _____

7. Сталкиваетесь ли Вы с трудностями в использовании АРМ / информационных систем и прочих автоматизированных технологий?

- да, часто;
- иногда;
- редко;
- никогда;
- Другое _____

8. Если да, то какие именно трудности у Вас возникают?

9. Проходили ли вы обучение / повышение квалификации по использованию информационных технологий в деятельности правоохранительных органов?

- да;
- нет;
- Другое _____

10. Как вы в целом оцениваете состояние информатизации правоохранительных органов?

- отличное;
- хорошее;
- удовлетворительное;
- плохое;
- Другое _____

Благодарим Вас за сотрудничество!

Результаты анкетирования

Опрошено: сотрудников Отдела дознания МВД по г. Челябинск – 25 человек

№	Вопрос	Варианты ответов	Результаты, (%)
1	Ваш возраст?	<input type="checkbox"/> до 25 лет <input type="checkbox"/> 26-30 <input type="checkbox"/> 31-40 <input type="checkbox"/> 41 и старше	8 % 60% 32 % 0 %
2	Какого уровня правоохранительный орган, в котором Вы работаете?	<input type="checkbox"/> федеральный; <input type="checkbox"/> региональный; <input type="checkbox"/> районный; <input type="checkbox"/> городской; Другое	100%
3	Сотрудником какого правоохранительного органа Вы являетесь?	<input type="checkbox"/> системы МВД РФ; <input type="checkbox"/> Прокуратура РФ; <input type="checkbox"/> СК РФ; <input type="checkbox"/> ФСБ; Другое	100%
4	Какую должность Вы занимаете?	<input type="checkbox"/> дознаватель	100%
5	Имеете ли Вы доступ к информационным технологиям (Автоматизированные рабочие места / Информационные системы / Технические средства)?	<input type="checkbox"/> да; <input type="checkbox"/> нет; Другое	100%
6	Как часто вы используете их в процессе своей профессиональной деятельности?	<input type="checkbox"/> всегда; <input type="checkbox"/> часто; <input type="checkbox"/> редко. <input type="checkbox"/> не использую совсем; Другое	72% 28%
7	Сталкиваетесь ли Вы с трудностями в использовании АРМ / информационных систем и прочих автоматизированных технологий?	<input type="checkbox"/> да, часто; <input type="checkbox"/> иногда; <input type="checkbox"/> редко; <input type="checkbox"/> никогда; Другое	32% 34% 34%
8	Если да, то какие именно трудности у Вас возникают?	сбой в программе; сбой в подключении; технического характера; нехватка специальных знаний;	

		частая смена паролей и логинов.	
9	Проходили ли вы обучение / повышение квалификации по использованию информационных технологий в деятельности правоохранительных органов?	<input type="checkbox"/> да; <input type="checkbox"/> нет; Другое	73% 27%
10	Как вы в целом оцениваете состояние информатизации правоохранительных органов?	<input type="checkbox"/> отличное; <input type="checkbox"/> хорошее; <input type="checkbox"/> удовлетворительное; <input type="checkbox"/> плохое; Другое	12% 20% 68%