МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени И.С. ТУРГЕНЕВА»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема выпускной квалификационной работы

«СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ»

Орел – 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность выбранной тематики выпускной квалификационной работы во многом обусловлена тем, что в настоящее время роль информационных технологий в жизни современного общества сопровождается высокими показателями повсеместного использования информационных ресурсов. Сложившееся цифровое общество характеризуется стремлением к упрощенной жизни, это обуславливается тем, что цифровизация способствует облегчению жизнедеятельности человека. Стремительные темпы усиливающихся потоков информации приводят к полной утрате существенных данных.

Компьютеризация и информатизация нашего общества в целом привели к формированию и возникновению наиболее развитых информационных технологий и новейших средств, которые при применении их, существенно упрощают расследование и раскрытие различного рода преступлений.

В современном мире с развитием научного и технического прогресса, информационные технологии являются существенной частью нашей жизни. Исходя из вышесказанного, можно отметить, что сегодня остаётся актуальным вопрос применения современных информационных технологий в раскрытии и расследовании преступлений сотрудниками правоохранительных органов.

Также, стоит отметить, что, к сожалению, не только органы государственной власти используют современные технические средства и технологии. Преступники также прибегают к новейшим техническим средствам для совершения преступных деяний их сокрытия. Преступления с использованиям новых информационных технологий можно отнести к трудно раскрываемым, так как, расследование подобных преступлений сопровождается рядом проблем.

Недостаток технологий, а также требуемых навыков в применении новейших технологий, имеют все шансы усложнить следствие по данным категориям преступлений.

Тем не менее, на основании целей и задач государства, направленных на внедрение цифровизации в различные сферы жизни и производства, Стратегия развития информационного общества, утвержденная президентом Российской Федерации, включает в себя переход от прежних установок к электронным форматам полиции, документооборота, а также правительства. И здесь информационные технологии занимают одно из центральных мест в деятельности органов внутренних дел РФ.

В связи с чем, актуализируется вопрос рассмотрения современного состояния, перспектив, а также проблемных вопросов использования информационных технологий в раскрытии и расследовании преступлений.

Степень научной разработанности темы.

Проблематика использования информационных технологий в раскрытии и расследовании преступлений имеет длительную исследовательскую историю. Значительный вклад в разработку различных аспектов использования информационных технологий в раскрытии и расследовании преступлений внесли такие исследователи как: Астафьева О.А., Бочарова Э.А., Валединская Е.Н., Закиров Р.Ф., Комардина А.А., Меняйло Д.В. и другие.

Помимо этого, стоит отметить, что вопрос использования информационных технологий в процессе совершения преступлений также уже достаточно длительный промежуток времени волнует юридическое сообщество, причем, как профессиональное, так и теоретическое.

В числе учёных, которые активно изучают данную тему под призмой своих научных изысканий, входят такие представители юриспруденции, как А.А. Лаврушкина, А.А. Ларинков, А.В. Маилян, Е.Н. Рязанова, М.А. Степанова, Р.Р.Хасанов, Е.В. Царёв, В.А. Шиплюк и многие другие.

Объектом данного исследования являются общественные отношения, возникающие в процессе использования информационных технологий в раскрытии и расследовании преступлений.

Предметом исследования выступают положения Конституции Российской Федерации, уголовного законодательства Российской Федерации, иных нормативно правовых актов и научные концепции, раскрывающие специфику использования информационных технологий в раскрытии и расследовании преступлений.

Цель работы заключается в комплексном исследовании современного состояния и перспектив использования информационных технологий в раскрытии и расследовании преступлений.

Для достижения указанной цели ставятся следующие **задачи**:

1) определить понятие «информационные технологии» и «информационное обеспечение» в раскрытии и расследовании преступлений;

2) рассмотреть информационные технологии, применяемые сотрудниками правоохранительных органов при раскрытии и расследовании преступлений;

3) выявить перспективы использования новых информационных технологий в раскрытии и расследовании преступлений;

4) исследовать возможность использования современных информационных технологий для предупреждения и пресечения преступлений;

5) обозначить основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационных технологий;

6) предложить пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений.

Методологическую основу написания выпускной квалификационной работы составили диалектический метод научного познания, общенаучные и

частнонаучные методы теоретического анализа, такие, как логический, сравнительно-правовой и формально-юридический.

Теоретическую основу составили труды учёных в области оперативно-розыскной деятельности, криминалистики, уголовного процесса, философии, информатики, программирования и др.

Эмпирическая база работы представлена результатами изучения уголовных дел, совершённых с использованием современных информационных технологий; уголовных дел в процессе расследования которых применялись информационные технологии; статистические исследования, содержащиеся в ведомственных информационных письмах и обзорах МВД России.

Теоретическая значимость работы. Проведенное исследование современного состояния, перспектив, а также проблем использования информационных технологий в раскрытии и расследовании преступлений, а также выводы и предложения, сформулированные по его результатам, вносят определённый вклад в развитие теории и практики следственных действий и оперативных мероприятий.

Практическая значимость работы состоит в том, что предложенные в работе пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений могут быть использованы при составлении научно-обоснованных рекомендаций сотрудникам правоохранительных органов по использованию информационных технологий в раскрытии и расследовании преступлений.

Апробация результатов исследования. Положения магистерской диссертации обсуждались на заседании кафедры уголовного процесса и прокурорского надзора Орловского государственного университета имени И.С. Тургенева, а также нашли отражение в статье: Современные возможности раскрытия и расследования преступлений по электронным следам [Электронный ресурс] // Теория и практика современной науки. –

2022. – №10(88) (дата публикации: 03.10.2022). – URL: https://www.modern-j.ru/_files/ugd/b06fdc_45e3021f444b45eeb9ddef48dc0a44c6.pdf?index=true.

Научная новизна исследования определяется его целью, задачами и проявляется в комплексном исследовании современного состояния и перспектив применения современных информационных технологий в раскрытии и расследовании преступлений, а также предложениями по усовершенствованию организации и управления процессом расследования преступлений с использованием информационных технологий.

Положения, выносимые на защиту:

1. Понятие «информационное обеспечение» в современном российском законодательстве не закреплено. Нет единого подхода к трактовке данного термина и среди учёных. Одни учёные считают, что при определении понятия «информационное обеспечение» следует применять технические термины, по мнению других в содержании понятия «информационное обеспечение» должно содержаться решение задач оперативно-розыскной деятельности. На наш взгляд, при определении информационного обеспечения предварительного расследования стоит говорить о конкретном наборе инструкций и данных, позволяющих решать такие вопросы как: выбор субъектов сбора информации, их компетенции; определение сроков, порядка и способов получения, фиксации, обработки и систематизации получаемой информации; анализ информации в рамках определенной процедуры с применением типовых методик и привлечением соответствующих специалистов; организация использования результатов анализа информации в практической деятельности органов предварительного следствия.

2. В настоящее время существует потребность в официальном разъяснении такого оперативно-розыскного мероприятия как «получение компьютерной информации», а также в систематизации механизма получения компьютерной информации, поскольку сейчас существуют значительные трудности применения его в практической деятельности

оперативно-разыскными органами. Перспектива применения оперативно-разыскного мероприятия «получение компьютерной информации» является высокой в связи с развитием компьютерных технологий и активного применения их в преступной сфере.

3. Представляется целесообразным закрепить в законодательстве право привлекать к участию в процессуальных действиях при проведении изъятия электронных носителей информации сотрудников не государственных организаций, специализирующихся на информационной безопасности, что позволит не отвлекать экспертов от выполнения компьютерно-технических судебных экспертиз;

4. В действующем Федеральном законе «О связи» установлены недостаточные сроки хранения электронной информации в финансово-кредитных учреждениях, у операторов платежных систем и операторов сотовой связи. Решение данной проблемы видится в реализации положений ст. 64 Федерального закона от 7 июля 2003 г.№ 126-ФЗ «О связи», в соответствии с которыми операторы связи обязаны хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий, а текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

5. В настоящее время в субъектах Российской Федерации нет единого подхода в отношении квалификации однотипных преступлений в сфере информационных технологий, что приводит к противоречиям правоприменительной практики. Исходя из этого, существует объективная необходимость в принятии Постановления Пленума Верховного Суда

Российской Федерации по делам о преступлениях в сфере информационных технологий.

Структура работы соответствует задачам и внутренней логике исследования и включает в себя введение, две главы, заключение, список литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

1.1. Понятия «информационное обеспечение» и «информационные технологии» в раскрытии и расследовании преступлений

Современный мир характеризуется активным развитием различных инновационных технологий и их внедрением во все сферы деятельности человека. Сейчас все страны мира, в том числе, Российская Федерация создают глобальное информационное общество с развитой системой инфокоммуникаций. В связи с чем, в России в последние годы был принят ряд нормативно-правовых актов, регламентирующих процесс внедрения различных информационных технологий во все сферы социально-экономической жизни. Можно отметить такие законодательные акты как: федеральный закон «Об информации, информатизации и защите информации», «Об электронной цифровой подписи»[1] и ряд других.

Все они базируются на положениях основного закона страны – Конституции Российской Федерации. Так, статья 29 Конституции РФ гарантирует, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»[2].

Особенно актуальным внедрение современных информационных технологий является для сотрудников правоохранительных органов. Взаимообмен служебно-справочной информацией с помощью современных информационных технологий оптимизирует работу сотрудников

[1] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // Собрание законодательства РФ", 11.04.2011, N 15, ст. 2036. Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5306.

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/.

правоохранительных органов, а также помогает более эффективно бороться с преступностью. В настоящее время происходит увеличение количества различных преступлений, в том числе «труднораскрываемых» расследование которых значительно упрощается при использовании современного информационного обеспечения и современных информационных технологий.

Исходя из этого, начать исследование в данной выпускной квалификационной работе представляется рациональным с определения понятий «информационное обеспечение» и «информационные технологии».

Так, термин «информационное обеспечение» нередко встречается в научной литературе. В.И. Даль трактует «обеспечение» как: «дать что-либо верное, снабжение чем-либо»[1].

В Большой советской энциклопедии можно встретить следующее определение: «информационное обеспечение – это обслуживание специалистов необходимой научной, технической и иной информацией, осуществляемое информационными службами и органами для ее дальнейшего использования»[2].

Анализ специализированной литературы показал, что определение информационного обеспечения с юридической точки зрения определяется характером и видом этой деятельности. Например, при раскрытии и расследовании преступлений, информационное обеспечение представляет собой определённую деятельность субъектов уголовного процесса.

Однако единого мнения относительно определения понятия «информационное обеспечение» в юридической литературе нет.

Так, например, В.Ю. Голубовский определяет информационное обеспечение оперативно-розыскной деятельности как «деятельность подразделений и служб органов внутренних дел (оперативных и

[1] Даль В.И. Толковый словарь живого великорусского языка : избр. ст. / В.И. Даль; совмещ. ред. изд. В.И. Даля и И.А. Бодуэна де Куртенэ. – М.: Олма-Пресс: Крас. пролетарий, 2004. С. 156.

[2] Большая советская энциклопедия. Том 10. Ива - Италики. 3-е изд. / Глав. ред. А. М. Прохоров. – М.: Сов. энциклопедия, 1972. С. 298.

неоперативных), направленная на получение из гласных и негласных источников оперативно значимых сведений, их хранение, обработку, передачу и использование в целях выявления, предупреждения, раскрытия и расследования преступлений»[1].

В то время, как А.М. Ишин полагает, что «информационное обеспечение – это, прежде всего, совокупность единой системы сбора и получения информации из внешних и внутренних источников, схем информационных потоков, циркулирующих в ходе раскрытия и расследования преступлений, а также методология использования имеющихся баз данных и построения новых баз данных»[2].

Отсутствие легального определения понятия «информационное обеспечение» создаёт определённые трудности его применения в раскрытии и расследовании преступлений. В современном мире, где информация выступает главным ресурсом, необходимо предусмотреть на законодательном уровне все возможные механизмы её получения. В частности, для возможности применять информационное обеспечение при раскрытии и расследовании преступлений, необходимо закрепить понятие «информационное обеспечение» в нормативно-правовом акте.

На наш взгляд, при определении информационного обеспечения предварительного расследования стоит говорить о конкретном наборе инструкций и данных, позволяющих решать такие вопросы как:

– выбор субъектов сбора информации, их компетенции;

– определение сроков, порядка и способов получения, фиксации, обработки и систематизации получаемой информации;

---

[1] Голубовский В.Ю. Теория и практика информационного обеспечения оперативно-розыскной деятельности подразделений криминальной милиции: автореферат дис. ... доктора юридических наук: 12.00.09 / С.-Петерб. ун-т МВД РФ. – Санкт-Петербург, 2001. С. 40.

[2] Ишин А.М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. 2016. №4. С. 25.

– анализ информации в рамках определенной процедуры с применением типовых методик и привлечением соответствующих специалистов;

– организация использования результатов анализа информации в практической деятельности органов предварительного следствия.

Также, следует обратить внимание на то, что основная цель применения информационного обеспечения заключается в получении информации. В контексте рассмотрения вопроса о применении информационного обеспечения в раскрытии и расследовании преступлений, стоит учитывать, что получаемая информация – это, прежде всего, данные о лицах, совершивших преступление, а также предметах, фактах, событиях, процессах получаемые в соответствии с законами, касающимися правоохранительной деятельности, материально зафиксированные и систематизированные.

В современных условиях информационное обеспечение наряду с уже сложившимися средствами и методами может быть обеспечено на основе использования информационных технологий с применением возможностей СМИ и ресурсной базы Интернета[1].

Термин «информационные технологии» был введён академиком Виктором Глушковым, и определяется, как совокупность различных способов работы с информацией, реализующихся посредством сбора, обработки и передачи данных[2].

В настоящее время определение информационной технологии закреплено в ФЗ «Об информации, информационных технологиях и о защите информации». В указанном законе информационные технологии определяются как «процессы, методы поиска, сбора, хранения, обработки,

[1] Лаврик О.Л., Калюжная Т.А. Содержание понятий «информационное обеспечение», «информационное сопровождение», «поддержка научных исследований» как этапы информационного обслуживания ученых // Вестн. Том. гос. ун-та. Культурология и искусствоведение. 2020. №40. С. 310.

[2] Хлебников А.А. Информационные технологии (для бакалавров). М.: КноРус, 2016. С. 116.

предоставления, распространения информации и способы осуществления таких процессов и методов»[1].

В законе от 7 февраля 2011 г. № 3-ФЗ «О полиции» (ст. 11, гл. 1) определяется, что полиция в своей деятельности обязана использовать достижения науки и техники, современных технологий и информационных систем[2]. Полиция также обязана применять сети связи и современную информационно-телекоммуникационную инфраструктуру (п. 1 ст. 12. гл. 1). Полиция использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности (п. 3 ст. 12. гл. 1). Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных (п. 4 ст. 12. гл. 1).

Использование в деятельности информационных технологий значительно повышает эффективность работы правоохранительных органов, особенно с учётом роста прогрессивного информационного обмена.

Также, информационные технологии активно применяются в следственной практике[3]. Например, следователь при собирании доказательств подготавливает и редактирует различные процессуальные документы с помощью компьютера; при проведении осмотра места происшествия, следственного эксперимента или иных следственных

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448; Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5292.

[2] Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 21.12.2021) «О полиции» // Собрание законодательства РФ, 14.02.2011, № 7, ст. 900; Собрание законодательства РФ, 27.12.2021, № 52 (часть I), ст. 8983.

[3] Вехов В.Б. Основные направления использования компьютерных технологий в деятельности следователя // Информационная безопасность регионов. 2007. №1. С. 49.

действий применяются средства, способные сделать качественные цифровые фотографии, видеозапись. Помимо этого, специальные информационные технологии применяются при составлении фоторобота – современные программы содержат некую базу элементов лица, которая позволяет смонтировать наиболее точный портрет.

Помимо этого, с помощью компьютерной техники можно подготовить различные доказательственные документы, например, заключения экспертов, акты документальных ревизий, бухгалтерские и иные документы, созданные другими участниками уголовного процесса[1].

Также, следователи активно применяют различные базы данных для поиска необходимой информации при расследовании преступлений[2].

В процессе раскрытия и расследования преступлений, сотрудниками правоохранительных органов нередко используется глобальная система взаимосвязанных компьютерных сетей – Интернет. С помощью Интернета сотрудники правоохранительных органов могут оперативно получать всю необходимую и актуальную информацию, а также общаться с населением в режиме он-лайн[3].

Использование Интернета в правоохранительной деятельности сейчас является дискуссионной темой у многих юристов как учёных, так и практиков. Это связано с тем, что как носитель массово потребляемой информации он превратился в мощный инструмент психологического и нравственно-правового воздействия.

Как полагает Е.П. Ищенко «основная цель использования Интернета в расследовании преступлений – поиск и передача из сети необходимой

[1] Овсянников И.В. Доказательственное значение актов ревизий и документальных проверок // Вестник ВИ МВД России. 2012. №4. С. 38.

[2] Эмиров М.Б., Саидов А.Г., Рагимханова Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Дагестанского государственного университета. 2011. №2. С. 65.

[3] Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. – Москва: Издательство Юрайт, 2022. С. 365.

криминалистически значимой информации в целях ее последующей аналитической обработки»[1].

Деятельность сотрудников правоохранительных органов непосредственно связана с воздействием на психологию людей. Ввиду этого при производстве отдельных оперативно-розыскных мероприятий органами дознания применяются различные примы и методы психологического воздействия на лиц, представляющих оперативный интерес, в том числе, посредством Интернета. Целью данного воздействие является принятие лицом идеи, навязываемой правоохранительными органами, в которой они нуждаются, а так же формирование этим лицом своего поведения определённым образом.

Нужно учесть тот факт, что все оперативные мероприятия преследуют цель получения истинной информации, которая имеет оперативное значение и является основополагающей составляющей при раскрытии и расследовании уголовного дела. Как показывает практика, бывает сложно восстановить факты совершенного преступления, а так же лиц его совершивших, получить информацию, если преступление было совершенно, в условиях неочевидности. Это возможно только через показания свидетелей или участников преступления. Несомненно, лица виновные в совершении преступления отказываются от дачи правдивых показаний, или от дачи показаний вовсе. Это выражается в отказе участвовать в отдельных следственных действиях и оперативно-розыскных мероприятиях, что несомненно приводит к разногласиям между правоохранительными органами и виновным лицом.

В связи с чем, актуализируется вопрос своевременного распространения информации о преступлении и деятельности органов предварительного следствия по его раскрытию. Самым оперативным способом является размещение этой информации в Интернете.

[1] Ищенко Е.П., Топорков А.А. Криминалистика: учебник / под ред. Е.П. Ищенко. 2-е изд., испр., доп. и перераб. М.: КОНТРАКТ, ИНФРА-М, 2010. С. 416.

Данные действия предотвращают различные слухи и домыслы населения относительно конкретного уголовного дела и деятельности правоохранительных органов. Особенно важным это является в случае, если уголовное дело получило значительный резонанс в обществе.

Таким образом, в современном быстро развивающемся мире особенно важно внедрение в деятельность правоохранительных органов современных инновационных технологий с целью стимулирования эффективной деятельности по раскрытию и расследованию преступлений.

1.2. Информационные технологии, применяемые сотрудниками правоохранительных органов при раскрытии и расследовании преступлений

Итог расследования противоправных действий в большинстве своём находится в зависимости от размера важных криминалистических данных, какими в данный период обладает следователь, дознаватель или те лица, которые привлекаются к взаимодействию с сотрудниками ОВД.

С целью получения и обработки необходимых сведений при расследовании преступлений, в последнее время органами внутренних дел всё чаще и чаще используются информационные технологии, также сотрудники ОВД применяют в своей деятельности специализированное программное обеспечение.

В настоящее время основным способом собирания оперативно-розыскной информации является осуществление оперативно-розыскных мероприятий. В конце 2016 года к ОРМ (оперативно-розыскные мероприятия) присоединилось новое мероприятия – «Получение компьютерной информации»[1]. Однако, что именно подразумевается под получением компьютерной информации в Законе осталось без уточнения.

[1] Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ, 11.07.2016, № 28, ст. 4558.

Федеральный закон «Об информации, информационных технологиях и о защите информации» в ст. 2 даёт общее понятие информации – это сведения (сообщения, данные) независимо от формы их представления[1].

Понятие компьютерной информации закреплено в Уголовном кодексе Российской Федерации. Так, исходя из примечания 1 к ст. 272 Уголовного кодекса Российской Федерации «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[2].

Также, в теории оперативно-розыскной деятельности нет единого подхода к установлению сущности получения компьютерной информации. Например, В.И. Шаров считает, что «более правильно подразумевать под получением компьютерной информации лишь запрос на получение сообщений определенного абонента у провайдера, администрации мессенджеров и электронной почты, т.е. те действия, которые предполагались изначально по антитеррористическому пакету, в результате принятия которого появилось это оперативно-розыскное мероприятие»[3]. В то время как по мнению Е.С. Дубоносова при определении понятия «получение компьютерной информации» необходимо прибегать к технической терминологии, а также учитывать решение задач ОРД[4].

Таким образом, в настоящее время существует потребность в официальном разъяснении такого оперативно-розыскного мероприятия как «получение компьютерной информации», а также в систематизации механизма получения компьютерной информации, поскольку сейчас

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448; Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5292.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.09.2022) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954; Собрание законодательства РФ, 26.09.2022, № 39, ст. 6535.

[3] Шаров В.И. Оперативно-розыскные мероприятия в сети интернет // Общество и право. 2018. № 2 (64). С. 85.

[4] Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения // Известия ТулГУ. Экономические и юридические науки. 2017. №2-2. С. 26.

существуют значительные трудности применения его в практической деятельности оперативно-разыскными органами. Перспектива применения оперативно-разыскного мероприятия «получение компьютерной информации» является высокой в связи с развитием компьютерных технологий и активного применения их в преступной сфере.

Исходя из того, что современные технологии осуществления информационных процессов, создают специфическую реальность путём передачи изображения и различного рода сообщений – это не только существенным образом видоизменяют преступную жизнь и преступность в целом, но и открывает возможности с ней бороться и эти возможности нужно как можно быстрее и в полном объеме интегрировать в криминалистику.

Справочно-аналитическая деятельность при выявлении противозаконных действия содержит в себе разнообразные способы сохранения, обработки доказательственных данных в целях принятия разного рода процессуальных решений. Источники получения доказательственных данных могут быть различными:

а) информация или обращение о содеянном преступлении, либо информация о приготовлении преступного деяния;

б) итоги следственных действий, а также оперативно-розыскных мероприятий;

в) заключение специалистов;

г) сведения криминалистических учётов;

д) выводы экспертов;

е) сведения из СМИ (средства массовой информации);

ж) своевременная информация, которая предоставляется участниками уголовного процесса;

з) оперативные сводки, ориентировки;

и) иные уголовные дела[1].

[1] Лазарева В.А. Доказывание в уголовном процессе : учебник для бакалавриата и магистратуры / В. А. Лазарева. – 7-е изд., перераб. и доп. – М. : Издательство Юрайт, 2019. С. 179.

Следователю, перерабатывая большой объём разной информации, связанной с преступностью, необходимо выбирать самые важные сведения. Помимо этого сущность информационно-аналитической работы увеличивается при расследования многоэпизодных и групповых преступлений. В связи с чем, для более эффективной работы, следователь применяет в своей работе средства информационных технологий.

Рассмотрим современные информационные технологий, которые активно применяются сотрудниками правоохранительных органов при раскрытии и расследовании преступлений.

Одной из таких информационных технологий является справочно-правовая информационная система (СПИС). С учётом положений Федерального закона «Об информации, информационных технологиях и о защите информации», справочно-правовая информационная система может быть отнесена к информационным системам, реализованным в форме базы данных, содержащей организационно упорядоченную совокупность документов (нормативные акты, справочные и иные материалы). Как информационная система, СПИС представляет собой совокупность содержащейся в базах данных информации, технических, программных и иных технологических средств, предоставляющая доступ к информации (информационные услуги). Порядок создания, эксплуатации, предоставления доступа к информации определяется правообладателем с учетом требований законодательства[1].

В данный момент при применении сотрудниками правоохранительных органов СПИС при расследовании и раскрытии преступлений, у них есть возможность получения различного рода информации между характеристиками преступлений и групп для регионов: обширное исследование преступной связи среди городов России; формирование

[1] Максимова В.П. Формы, методы и направления использования специальных знаний в целях выявления и преодоления противодействия расследованию преступлений // Юридическая наука и правоохранительная практика. 2017. №3 (41). С. 199.

виртуального «мира» и составления плана раскрытия преступления; формирование виртуальных методических советов и рекомендаций, очередность различных решений, которые могут быть связаны с оперативно-розыскными задачами, а также следственными и экспертами[1].

Использование нынешних информационных технологий не только «рационализирует» движение, которые совершаются на данный период времени в уголовном судопроизводстве, но и трансформирует концепцию с целью решения различных задач, стоящих перед следователями и оперативными работниками органов внутренних дел Российской Федерации.

Также, для сотрудников правоохранительных органов, а именно следователей, дознавателей, оперативных работников, подсистемы современного информационного обеспечения очень полезны для того, чтобы:

– исследовать материалы многоэпизодного уголовного дела, где присутствуют два и более обвиняемых;

– исследовать необходимые сведение согласно комплексу уголовных дел, которые прежде были приостановлены по какому-либо основанию;

– исследовать необходимые сведения о документах и различных ценностях при раскрытии преступного деяния в различных сферах.

Также, сотрудники правоохранительных органов в своей деятельности применяют информационную систему «Спрут». Данная система решает важные задачи для расследования и раскрытия преступления, а именно осуществляет:

– усовершенствование работы сотрудников следственных отделов на стадии возбуждения уголовного дела;

– формирование учёта и контроля за раскрытием уголовных дел;

– формирование концепций, которые включают разнообразие методики для раскрытия и расследования уголовных дел;

[1] Салиев А.А. К понятию о роли специальных знаний используемых в ходе расследования преступлений // European journal of law and political sciences. 2016. №4. С. 78.

– формирование дактилоскопических учётов, а также закрепление и фиксация мест совершения преступного деяния для реконструкции с помощью схем.

Помимо этого, можно отметить программный комплекс «Гранд-УД», данный комплекс объединяет две подсистемы:

– автоматизированное рабочее место (АРМ) следователя;

– автоматизированное рабочее место (АРМ) руководителя.

Если говорить про АРМ следователя, то применение программного комплекса «Гранд-УД» может решить такие задачи, как:

– зафиксировать в базе данных процесс допроса или же очной ставки;

– сохранить различные фабулы совершённых преступлений;

– автоматизированное составление различных процессуальных документов;

– можно выделять движения каждого уголовного дела и тех лиц, которые проходят по данному делу;

– быстро найти любое уголовное дело, которое зарегистрировано в компьютере и любое лицо, которое проходит или проходило ранее по уголовному делу;

– осуществить планирование расследования по уголовному делу.

Информационно-рекомендующие системы содержат методики, которые в зависимости от конкретной ситуации, предлагают начинающему следователю или даже уже достаточно опытному, алгоритм следственных действий, где содержатся справочные материалы, которые достаточно часто применяет следователь при расследовании преступлений.

Также необходимо отметить, что АРМ следователя, содержат методики расследования преступлений в таких сферах, как:

– сфера компьютерной информации;

– сфера, связанная с незаконным оборотом наркотических средств и психотропных веществ;

– сфера, связанная с посягательством на культурные ценности;

– грабежи и разбойные нападения на граждан;

– квартирные кражи;

– пожары (поджоги);

– бандитизм и др.

Что касается АРМ руководителя, то оно позволяет создать учёт и соблюдать контроль за расследованием уголовных дел, а также решает такие задачи, как:

– контроль, за исполнением указаний;

– контроль основных данных по уголовным делам в порядке части четвертой, статьи тридцать девятой Уголовно-процессуального Кодекса Российской Федерации[1];

– сохранение в базе данных всех решений, которые принимает следователь по конкретному уголовному делу;

– сохранение запросов на поиск интересующего уголовного дела или лица, которое проходит или проходило по данному уголовному делу;

– процессуальные сроки следствия высчитываются автоматически;

– расчет сроков содержания под стражей происходит автоматически;

– ведение статистически следственной деятельности и определенной отчетности следователя конкретного подразделения.

Имеется также и подсистема архивов, которая предоставляет возможность поиска определённого круга лиц в архиве, поиска определённого субъекта для расследования того или иного уголовного дела.

Кроме того, специальная территориально-распределенная автоматизированная система позволяет найти организационное решение, процессуальные проблемы и задачи, которые сформированы к общей информационной сети ОВД РФ.

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 07.10.2022) // Собрание законодательства РФ, 24.12.2001, № 52 (ч. I), ст. 4921; Собрание законодательства РФ, 10.10.2022, № 41, ст. 6946.

Важно отметить и такую систему как – СТРАС-СК России. Совместно с подсистемой «расследования», данная система используется с целью поддержания следователя при решении процессуальных задач по уголовному делу[1]. Эта система выстроена на базе разных криминалистических методов при раскрытия преступного деяния.

Одним из значимых вопросов при расследовании преступления является осмотр места происшествия (ОМП), связи с этим, сотрудники ОВД стараются как можно чаще использовать современные технические средства при раскрытие преступления, а также при обнаружение различных улик и следов при ОМП.

В соответствии с этим максимальное формирование обретают «фотограмметрические» системы, которые гарантируют обычный стиль фотосъемки, кроме того, установление разных предметов и улик при ОМП. На базе «фотограмметрии» применяя нынешнюю графику, допустимо крайне отчетливо с помощью «фотограмметрии» преобразить целую ситуацию в правильности и точности. С целью решения данной задачи придумана концепция многомерного «пространственного» информационного моделирования места совершения преступления с воспроизведением динамики совершившегося преступления. Данная концепция, создана с целью построения места преступления на базе протокола его осмотра и при «фотограмметрической» съемки на базе «3D»[2].

Активное усовершенствование современных технологий расширяет спектр их применения в работе следователей и иных сотрудников ОВД. Опытнейшие следователи уже не первый раз практикуют переход с фотографий и стандартных видеозаписей, которые они производили на ОМП, в современную и цифровую форму с печатью кадров, которые могут иметь существенную значимость для раскрытия преступления.

---

[1] Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6. С. 179.

[2] Терехов А.М. Моделирования и прогнозирования преступности: теоретический аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. №2 С. 125.

Кроме того, в настоящее время используются современные видеокамеры и фотоаппараты нового поколения, которые дают возможность совершать и выводить разноцветные снимки в формате 3D, создавать своеобразную виртуальную анимацию.

Более важной основой доказательства для следователя и оперативного сотрудника, как мы выделяли прежде, станут криминалистические учеты, которые начали в настоящее время вестись при поддержке современных информационных технологий.

Также, на данный момент, мы можем выделить внедрения в систему дактилоскопической идентификационной системы «АДИС». На сегодняшний день, в нагрузке следователей присутствует огромный объём «дактилокарт» различных лиц, которые проходят по конкретному преступлению в уголовном деле, также и снятых следов при осмотре места происшествия. Для оптимизации работы с таким большим объёмом материалов применяется система «АДИС». Данная система представляет собой программно-технический комплекс, который применяется для учетов следов рук по лицам, которые проходят по уголовному делу или же которые ранее стояли на учете[1].

Для поставленных целей АДИС переходит на систему «Папилон», данная система применяется для полного и точного установления папиллярного узора. АДИС «Папилон» используют почти во всех регионах нашей страны, эта система отечественного производства, автоматизированная информационно-поисковая система, которая в свою очередь обеспечивает характеристики на любом объеме информации дактилокарты без отбора по их качеству[2].

Данная система обеспечивает:

– сохранение дактилокарт в конкретной основе сведений;

[1] Сафонов А.А. Современная автоматизированная дактилоскопическая идентификационная система органов внутренних дел российской федерации // Вестник экономической безопасности. 2021. №3. С. 180.

[2]

– сохранение фотоизображений;

– ведение специальных примет и описание людей по правилам так называемого «словесного портрета»;

– сохранение отпечатков пальцев рук, а также ладоней;

– обеспечение возможности поиска «карта-карта» для поиска определённой личности, «карта-след» для поиска следа, который был оставлен подозреваемым и изъят с места совершения преступного деяния, а также «след-след» с целью правильности определения самого факта совершения преступного деяния одним и тем же человеком;

– осуществление поиска следов и отпечатков ладоней;

– предоставление дактилоскопической информации к основной базе данных.

Сотрудниками правоохранительных органов также активно используется автоматизированная система «Квадрат», которая была разработана в информационном центре Управления Внутренних Дел Свердловской области. Система «Квадрат» даёт возможность установить зависимость между возрастом преступников и выбором места совершения преступления, причем по конкретным видам правонарушений[1].

Система предоставляет единый вид преступности в областном центре, её разделение согласно местности, а также может предоставить помощь в обнаружении зон преступления, где эти самые деяния совершаются определенными типами людей.

Исследование демонстрирует, из каких мест данной территории прибыли злоумышленники, к какой они возрастной категории относятся, с целью осуществления преступного плана или же куда с данной целью уезжали преступники.

[1] Ваценко А.А. Обзор техник компьютерной криминалистики // Бюллетень науки и практики. 2020. №6. С. 168.

Данная система предоставляет вероятность определить взаимосвязь между возрастной категории правонарушителей и подбором зон совершения конкретного преступного деяния.

Подводя итог, хочется отметить, что применение информационных технологий в раскрытии и расследовании преступлений приобретает всё большую актуальность в условиях модернизации всех сфер современной жизни. Использование современных технологий способствует оптимизации и повышению эффективности работы правоохранительных органов в раскрытии и расследовании преступлений.

1.3. Перспективы использования новых информационных технологий в раскрытии и расследовании преступлений

Сегодня деятельность сотрудников ОВД невозможна без применения новейших IT-технологий, поскольку совершенствование информационного обеспечения напрямую зависит от технической оснащенности Министерства внутренних дел РФ. Роль новейших информационных технологий заключается в эффективном и быстром решении служебных задач, возложенных на правоохранительные органы, а именно раскрытие и расследование преступлений. Департамент информационных технологий, связи и защиты информации МВД России, созданный в 2011 году, определяет основные способы совершенствования технической базы государства и цифровых систем связи, регулирует вопросы разработки ведомственных проектов в сфере информатизации[1].

Основным документом, определяющим направления развития информационного общества в России, является Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы[2].

[1] Приказ МВД России от 15.06.2021 № 444 (ред. от 28.12.2021) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

[2] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ, 15.05.2017, № 20, ст. 2901.

Исходя из Стратегии, внедряются в обиход и широко используются такие понятия как «цифровая полиция» и «цифровой полицейский». «Цифровая полиция» определяется, как система подразделений ОВД РФ, осуществляющая свою деятельность посредством активного применения перспективных информационных технологий для достижения поставленных задач в едином цифровом пространстве[1].

Перспективные задачи реализации Стратегии раскрыты в Программе – Цифровая экономика[2]. Представляется очевидным, что цифровая экономика не ограничивается сферой бизнеса. Развитие информационного общества затрагивает все ключевые аспекты жизни общества, в том числе правоохранительный сегмент. Цифровизация экономики предъявляет новые требования к научно-технической деятельности, обеспечивающей повышение эффективности выполнения оперативно-служебных задач и осуществления полномочий, возложенных на МВД России. Так, в соответствии с Распоряжением МВД России «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022-2024 годы», ФКУ НПО «СТиС» МВД России было поручено инновационное развитие специальной техники, специальных информационно-коммуникационных технологий и средств связи[3].

Усовершенствованные СТиС и СВ реализуются за счет использования аппаратно-программных средств, которые, в свою очередь, базируются на основе цифрового принципа представления информации.

---

[1] Сухов А.В., Конюшев В.В. Цифровая полиция как эргатическая система, функционирующая в цифровой экосистеме // Правовая информатика. 2021. №2. С. 29.

[2] Постановление Правительства РФ от 02.03.2019 № 234 (ред. от 13.05.2022) «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с "Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации») // Собрание законодательства РФ, 18.03.2019, № 11, ст. 1119; Собрание законодательства РФ, 23.05.2022, № 21, ст. 3443.

[3] Распоряжение МВД России от 11.01.2022 № 1/37 (ред. от 30.06.2022) «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022-2024 годы» // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

Наиболее подробно требуется рассмотреть направления развития СТиС и СВ на современном этапе становления инновационной структуры органов внутренних дел[1].

1. Сегодня информационно-коммуникационные технологии МВД России основываются на внедрении технологий «искусственного интеллекта». Благодаря этому, в будущем есть возможность повышения эффективности раскрытия преступлений. Данное внедрение в практику также должно быть направлено на защиту граждан от преступных посягательств.

2. Обеспечение способности общения подразделений полиции с гражданами в условиях ЧС.

3. Установление лиц, подозреваемых в совершении преступления, по биометрическим данным.

4. Детекция и механическое блокирование потенциальных угроз, которые создают опасность для жизни населения.

5. Возможность самостоятельной работы ТС, либо с помощью программы использования.

6. Электронная передача важной информации и срочных распоряжений сотрудников полиции гражданской робототехнике.

7. Оснащение служебных технических средств сотрудников полиции новыми комбинированными установками.

8. Наблюдение за определенным объектом с одновременным использованием подсистем ПРТС на любой территории.

9. Ведение беспрерывного надзора с помощью применения робототехники (аудио-, видео-охват) за всеми передвижениями

[1] Созаева А.С. Использование новых информационных технологий в раскрытии и расследовании преступлений // В сборнике: Право в эпоху информационных технологий: проблемы и пути решения. Сборник материалов международной научно-практической конференции среди студентов, магистрантов и аспирантов. Пермь, 2021. С. 202.

наблюдаемого объекта, транспортных средств, и передача собранной информации в пункт управления полицией[1].

Все предложенные сферы развития средств связи и наблюдения целенаправленно определяют курс развития, сопровождающийся созданием оперативных модулей информационного воздействия на уголовное судопроизводство. Создание стандартного проекта технического оснащения гарантирует автоматизирование действий сотрудников ОВД РФ, то есть при этом все возложенные на них функциональные обязанности должны будут обеспечиваться реализацией унификации экранных форм, предоставлением информации в виде досье, а также введением Системы сторожевого контроля, которая обладает наступательной стратегией в борьбе с преступностью.

Единая информационно-телекоммуникационная система (далее ЕИТКС) в системе МВД необходима для создания и построения целостного аналитического механизма, направленного на обеспечение базового уровня оснащения техническими средствами подразделений органов внутренних дел. Крупные информационные системы ГЛОНАСС[2] и Аппаратно-программный комплекс «Безопасный город»[3] созданы для предупреждения возможных угроз, которые могут отразиться на общественной безопасности.

Необходимо отметить, на сегодняшний день в линии МВД РФ включается 48 информационных услуг, которые в полной мере преобразованы в электронный формат. Но Министерство предоставляет лишь 5 действительно необходимых. Теперь граждане нашей страны могут обращаться в правоохранительные органы не только лично и по телефону, но еще и с помощью интернета. Важным моментом является тот факт, что

[1] Бецков А.В. О научно-технической политике мвд россии до 2030 года // НиКа. 2020. №. С. 28.

[2] Постановление Правительства РФ от 25.08.2008 №641 (ред. от 12.11.2016) «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» // Собрание законодательства РФ, 01.09.2008, № 35, ст. 4037; Собрание законодательства РФ, 21.11.2016, № 47, ст. 6640.

[3] Распоряжение Правительства РФ от 03.12.2014 № 2446-р (ред. от 05.04.2019) «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // Собрание законодательства РФ, 15.12.2014, № 50, ст. 7220; Собрание законодательства РФ, 15.04.2019, № 15 (часть IV), ст. 1803.

начальные стадии автоматизации технического обеспечения полиции берут свое начало еще в 70-х годах прошлого века.

Сначала электронная вычислительная машина Минск-22 и 32, чуть позднее ЭВМ типа ЕС и СМ – не позволяли единой информационной базе полностью реализоваться как на региональном, так и на федеральном уровне. Поэтому сейчас компьютеризация органов внутренних дел характеризуется переоснащением информационных центров в пользу суперсовременных систем для зонального и регионального уровня.

По большому счету, сейчас в системе Министерства внутренних дел Российской Федерации совершенствуется режим ЭВМ, который обеспечивает быстрое выполнение задач оперативно-розыскного и учетно-статистического характера[1].

Информационный подход к решению уголовно-процессуальных задач является одним из преобладающих методов приема и использования полученной совокупности сведений. А.Р. Белкин в учебном пособии «Теория доказывания в уголовном судопроизводстве» выделяет роль информационных технологий в раскрытии и расследовании преступлений, а также отмечает важность получения информации о событии преступления, которая изначально является предметом доказывания[2]. Как говорилось ранее, с целью внедрения электронного документооборота в уголовно-процессуальную деятельность необходимо: широко использовать электронную подпись; массово развивать реализацию процессуальных действий без реального присутствия участников уголовного судопроизводства; осуществлять защиту свидетелей и иных лиц в электронном формате; активно применять инновационные средства контроля.

---

[1] Комардина А.А., Меняйло Д.В., Меняйло Л.Н. Применение информационных технологий и возможностей цифровизации в деятельности сотрудника ОВД // В сборнике: Экономическая безопасность: правовые, экономические, экологические аспекты. Сборник научных трудов 6-й Международной научно-практической конференции. Курск, 2021. С. 185.

[2] Белкин А.Р. Теория доказывания в уголовном судопроизводстве. В 2 ч. Часть 2: учеб. пособие для вузов / А. Р. Белкин. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2019. С. 163.

Выгодная разработка эффективных методов, позволяющих перестраивать индивидуальные признаки внешнего облика человека, реализуется за счёт разработки портретов преступника. По той причине, что ручные системы поиска уже потеряли свою прежнюю актуальность, и в полной мере не способны оперативно представлять точную информацию, и на поиск сведений затрачивается много времени, то применение современных информационных технологий является значимым направлениям развития IT-технологий в органах внутренних дел.

Создание крупных баз данных сопровождается быстрым поиском важной информации, необходимой для раскрытия и расследования преступлений, в особенности по горячим следам. К наиболее часто используемым следует отнести габитоскопические системы и системы, которые позволяют установить личность. Важно отметить, что высокий коэффициент раскрываемости преступлений зависит не от наличия технических средств в ОВД, именно от качества их применения[1].

Расследование преступлений может обеспечиваться универсальным и специальным программным обеспечением, первое – осуществляется посредством использования сетевых технологий, оптических средств распознавания знаков и символов, текстовых процессоров; второе – путем применения IT-технологий, направленных на решение конкретной задачи. В качестве примера автоматизированной системы управления можно привести АСУ «Дежурная часть», управляющая службами МВД во время реагирования на преступление. Система АБД активно используются правоохранительными органами.

Автоматизированный банк данных включает в себя четкую информацию о нераскрытых преступлениях; похищенном или утерянном оружии, боеприпасов; предметах и вещах, имеющих регистрацию и

[1] Страхов А.А., Слесарева Е.А., Задохина Н.В. Информационные технологии в ОВД. Основные термины и определения: словарь / М.: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. С. 101.

соответственно индивидуальные номера. Из федерального проекта «Цифровое государственное управление» стало известно, что 22 ноября 2021 года Российская Федерация выделила около 40 млрд. руб. на развитие информационной инфраструктуры государства[1]. В рамках данного проекта также планируется обновление идентификационного документа гражданина, который будет содержать электронный носитель информации. Также до 25 декабря 2024 года планируется разработка ИИ-системы поиска серийных преступников и определения их внешности с помощью генетического материала. Данная технология будет способствовать анализу сразу нескольких преступлений.

Реализация намеченных планов позволит нашей стране выйти в первые ряды лидеров российской науки, а также МВД предполагает тем самым повысить раскрываемость преступлений и правонарушений. На основе рассмотрения роли информационных технических средств в деятельности правоохранительных органов можем прийти к выводу о том, что в настоящее время IT-технологии занимают одно из ведущих мест в системе расследования и раскрытия преступлений, повышение качества и эффективности служебной деятельности напрямую зависит от их применения. На данном этапе техническая база ОВД РФ полностью не оснащена, что говорит о необходимости постоянного совершенствования способов и методов раскрытия преступлений.

В настоящее время в Российской Федерации совершается значительное количество хищений. Каждый день оперативными подразделениями полиции территориальных органов регистрируются заявления граждан по фактам краж, грабежей, разбоев. Большинство преступлений происходит на улицах городов и иных населённых пунктов. При осуществлении мероприятий по раскрытию данного вида преступлений сотрудники органов внутренних дел

[1] Паспорт федерального проекта «Цифровое государственное управление» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/.

используют комплекс оперативно-розыскных, уголовно-процессуальных и тактических мероприятий[1].

Перечислим некоторые из них:

Опрос – это оперативно-розыскное мероприятие, представляющее собой специальную беседу сотрудника оперативного подразделения с гражданами, которые располагают или могут располагать информацией, представляющей определенный интерес для органов, осуществляющих оперативно-розыскную деятельность[2].

Опрос важен при получении первичной информации о преступлении. Насколько качественно он будет проведён сотрудником полиции, настолько успешным будет раскрытие каждого хищения. Проводится с потерпевшими, очевидцами, иными лицами способными дать информацию по конкретному преступлению. Осмотр места происшествия, местности, жилища, иного помещения, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для раскрытия преступления и, в дальнейшем, для успешного расследования уголовного дела.

Отождествление личности – оперативно-розыскное мероприятие, позволяющее в непроцессуальной форме идентифицировать подозреваемых лиц по статическим или динамическим признакам внешности (например, по походке, мимике, жестикуляции). Речь идет о ситуации, которая в оперативно-розыскной работе встречается довольно часто – необходимо опознать представляющее интерес лицо лично, или же по фотографии, субъективному портрету, рисованному портрету, по видеоизображению, дабы сравнить с подозреваемым.

---

[1] Малышева И.В. Использование современных информационных технологий в деятельности оперативных подразделений полиции при раскрытии имущественных преступлений // В сборнике: Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы международной научно-практической конференции. Составитель Э. Х. Мамедов. 2019. С. 575.

[2] Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 28.06.2022) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ, 14.08.1995, № 33, ст. 3349; Собрание законодательства РФ, 04.07.2022, № 27, ст. 4603.

Проверка на причастность лиц, привлекаемых ранее за совершение аналогичных преступлений – осуществление проверки по месту жительства или иного места пребывания граждан, состоящих на профилактическом учёте в органах внутренних дел, совершивших ранее аналогичные преступления[1].

Снятие информации с технических каналов связи – оперативно-розыскное мероприятие, заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям. В настоящее время данное мероприятие особенно актуально, так как большинство мест в современных населённых пунктах оборудованы видео камерами, и процедура раскрытия преступления часто зависит от информации, полученной с данных технических средств наблюдения. Сложенная воедино информация, полученная в результате вышеперечисленных действий, ложится в основу уголовного дела и от её качества и полноты, заключающихся в подробном описании примет подозреваемых, перечня похищенного, особенностей совершения преступления, мест возможного нахождения подозреваемых и похищенного и др., зависит будет ли раскрыто каждое конкретное преступление, и будут ли виновные привлечены к ответственности[2].

Необходимо отметить, что ранее оперативные подразделения органов внутренних дел при осуществлении розыска лиц, подозреваемых в совершении хищений, имели весьма ограниченный перечень действий по выявлению данных преступлений. Они заключались в проведении опросов, осмотров места происшествия, работы по получению информации от спецаппарата (лиц, оказывающим содействие оперативным подразделениям на добровольной основе).

---

[1] Приказ МВД России от 17.01.2006 № 19 (ред. от 28.12.2021) «О деятельности органов внутренних дел по предупреждению преступлений» (вместе с «Инструкцией о деятельности органов внутренних дел по предупреждению преступлений») // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

[2] Демидченко Ю.В. Снятие информации с технических каналов связи как один их способов получения сведений, используемых в процессе доказывания по уголовному делу // Вестник юридического факультета Южного федерального университета. 2021. №4. С. 65.

Возможности привлечения технических средств к раскрытию данных преступлений были очень ограничены, так как в основном были задействованы для нужд подразделений аппаратов управлений территориальных органов ОВД, сотрудники же низовых оперативных подразделений полиции осуществляя раскрытие данных преступлений, опирались исключительно на собственное мастерство и знание оперативной обстановки на подведомственном участке деятельности. Также, для использования технических средств требовалось большое количество согласований с вышестоящим руководство, а уличные преступления эффективно раскрываются «по горячим следам», где дорога каждая минута.

В современных условиях оперативные подразделения полиции могут использовать многочисленные социальные контенты, которые в большом количестве представлены в сети Интернет. Большинство подразделений полиции имеют выход в глобальную сеть и способны использовать её мощности для осуществления розыскных мероприятий. Помимо этого, развитие информационных технологий шагнуло настолько далеко, что каждый гражданин, в том числе сотрудник полиции, имеет в пользовании телефон с выходом во всемирную информационную сеть, а в некоторых подразделениях присутствует практика выдачи данных устройств в служебное пользование[1].

Иными словами, современные сотрудники оперативных подразделений полиции могут свободно пользоваться возможностями «всемирной паутины» в оперативно-розыскных целях. При розыске лиц, подозреваемых в совершении грабежей, разбоев, когда необходимо выявить лиц, подозреваемых в данных преступлениях и при наличии данных, полученных с видеокамер, возможно действовать следующим образом. При наличии видеозаписи, на которой виден подозреваемый в совершении данного

[1] Токбаев А.А., Кудрявцев С.В., Несмелов П.В. Применение информационных технологий в деятельности ОВД // В сборнике: Актуальные вопросы тактико-специальной подготовки сотрудников правоохранительных органов. Сборник статей предназначен для научных работников, педагогических работников, курсантов и слушателей образовательных организаций системы МВД России Сборник статей по итогам научно-практической конференции под редакцией В.Н. Гонтаря. 2020. С. 110.

преступления, возможно вычленить фото, и при помощи специальных информационных программ попробовать запустить через фильтр социальных сетей и, таким образом, установить личность подозреваемого лица. Далее, путем проведения оперативно-розыскного мероприятия «Отождествление личности» целесообразно установить тот ли это действительно гражданин со слов потерпевшего, и при получении подтверждающей информации возможно продолжения работы по привлечению к уголовной ответственности путём применения уголовно-процессуального законодательства после организации процедуры опознания[1].

При осуществлении мероприятий по розыску похищенных вещей необходимо и целесообразно использовать такие сайты как «Авито», «Юла», с использованием которых подозреваемые могут сбывать добытое преступным путём имущество. По описанию, данным потерпевшими, на сайтах возможно обнаружить похищенные вещи, чтобы изъять их процессуальным способом (протокол выемки, изъятия и т. д.).

Когда данные подозреваемого в совершении хищения известны, возможно при помощи специальных программ, установить его место нахождение при помощи анализа страниц в социальных сетях. При невозможности его обнаружить сразу, возможен выход в социальную сеть под вымышленными данными и путём осуществления легендированной оперативной игры в сети Интернет, попытаться выманить его с последующей целью задержания.

Подводя итог, хочется отметить, что современные информационные технологии позволяют оперативным подразделениям полиции достичь эффективных результатов в области раскрытия преступлений имущественной направленности. При этом эти возможности всегда под

[1] Фетисов А.В., Никитин Д.В. К вопросу использования современных специальных средств с применением информационных технологий в деятельности ОВД // В сборнике: Современные подходы к подготовке сотрудников ОВД к действиям при возникновении чрезвычайных обстоятельств. Сборник научных статей реферативных чтений, посвящённых дню Российской науки кафедры ДОВД в ОУ УНК СП Московского университета МВД России имени В.Я. Кикотя. Под общей редакцией В.Н. Гонтаря. 2019. С. 197.

рукой и не требуют длительных согласований с вышестоящими инстанциями. Главная задача при этом – использовать максимальный ресурс сети Интернет с целью получения результатов в ходе оперативно-розыскных мероприятий.

Вывод по главе:

Исследуя теоретические основы использования информационного обеспечения и информационных технологий в раскрытии и расследовании преступлений, удалось сформировать такие понятия как «информационные технологии» и «информационное обеспечение».

Так, под информационными технологиями в действующем законодательстве Российской Федерации понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Данное определение закреплено в Федеральном законе «Об информации, информационных технологиях и о защите информации».

Понятие «информационное обеспечение» в современном российском законодательстве не закреплено. Нет единого подхода к трактовке данного термина и среди учёных. Одни учёные считают, что при определении понятия «информационное обеспечение» следует применять технические термины, по мнению других в содержании понятия «информационное обеспечение» должно содержаться решение задач оперативно-розыскной деятельности.

На наш взгляд, при определении информационного обеспечения предварительного расследования стоит говорить о конкретном наборе инструкций и данных, позволяющих решать такие вопросы как: выбор субъектов сбора информации, их компетенции; определение сроков, порядка и способов получения, фиксации, обработки и систематизации получаемой информации; анализ информации в рамках определенной процедуры с применением типовых методик и привлечением соответствующих

специалистов; организация использования результатов анализа информации в практической деятельности органов предварительного следствия.

Рассматривая информационные технологии, которые в настоящее время применяются сотрудниками правоохранительных органов при раскрытии и расследовании преступлений, удалось выявить следующие:

1) Справочно-правовая информационная система (СПИС);
2) Программный комплекс «Гранд УД»;
3) Дактилоскопическая идентификационная система «АДИС»;
4) Автоматизированная система «Квадрат».

Нами были рассмотрены самые эффективные и широко применяемые правоохранительными органами инновационные средства для раскрытия и расследования преступлений, однако это далеко не все. В современном мире рименение информационных технологий в раскрытии и расследовании преступлений приобретает всё большую актуальность в условиях модернизации всех сфер современной жизни. Использование современных технологий способствует оптимизации и повышению эффективности работы правоохранительных органов в раскрытии и расследовании преступлений.

Определяя перспективы использования новых информационных технологий в раскрытии и расследовании преступлений удалось прийти к выводу о том, что на сегодняшний день самым перспективным является внедрение технологий «искусственного интеллекта». Благодаря этому, в будущем есть возможность повышения эффективности раскрытия преступлений. Данное внедрение в практику также должно быть направлено на защиту граждан от преступных посягательств. Помимо этого, сейчас в системе Министерства внутренних дел Российской Федерации совершенствуется режим ЭВМ, который обеспечивает быстрое выполнение задач оперативно-розыскного и учетно-статистического характера. Реализация намеченных планов позволит нашей стране выйти в первые ряды лидеров российской науки, а также МВД предполагает тем самым повысить раскрываемость преступлений и правонарушений.

ГЛАВА 2. ПРОБЛЕМНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

2.1. Использование современных информационных технологий для предупреждения и пресечения преступлений

Одной из основных целей деятельности правоохранительных органов является успешное раскрытие преступлений. Современные информационные технологии выступают значимым инструментов в достижении этой цели. Однако для обеспечения безопасности государства и общества важно не только раскрыть преступления и наказать виновных, важно предотвратить совершения преступлений в будущем[1].

Поскольку сейчас общество всё больше становится информационным, новейшие технологии становятся основным средством для предупреждения и пресечения преступлений. Инновационные технологии позволяют сотрудникам правоохранительных органов оперативно получать следовую информацию, которая не только способствует успешному раскрытию преступлений, но и позволяет пресекать совершение преступлений.

Так, автоматизированная информационная система «Безопасный город», утверждённая распоряжением Правительства РФ в 2014 году позволяет выявлять и пресекать преступления[2].

В данной автоматизированной системе создаётся центр обработки и хранения информации из полученных источников видеофиксации. На основе этих данных программа может зафиксировать, например, массовые скопления граждан и составить прогноз возможных очагов возникновения

[1] Антонян Ю.М. Общая концепция предупреждения преступности // Человек: преступление и наказание. 2013. №3. С. 18.

[2] Распоряжение Правительства РФ от 03.12.2014 № 2446-р (ред. от 05.04.2019) «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // Собрание законодательства РФ, 15.12.2014, № 50, ст. 7220.

массовых беспорядков и дать сигнал для направления туда патрульных экипажей с целью пресечения массовых беспорядков[1].

Процесс внедрения АИС «Безопасный город» активно распространяется как в крупных городах, так и в городах с небольшим населением граждан. Применение данной системы позволяет предупреждать преступления и нарушения общественного порядка.

Так, 29 марта 2021 года Дымшаков И.А., находясь в общественном месте, в помещении магазина «Перекрёсток» – «умышленно, из хулиганских побуждений, грубо нарушая общественный порядок, выражая явное неуважение к обществу, желая противопоставить себя окружающим и продемонстрировать своё пренебрежительное отношение к ним, используя малозначительный повод, с целью применения насилия посредством использования вышеуказанного пистолета к ранее ему незнакомому Половинко А.В., находясь вблизи других граждан, достал указанный пистолет и, применяя его в качестве оружия, направил в сторону "ПАВ", и произвел несколько выстрелов из пневматического пистолета марки ПМ-49 в "ПАВ"»[2].

Благодаря установленной в магазине видеофиксации АИС «Безопасный город», сотрудники правоохранительных органов смогли оперативно отреагировать на данное противоправное действие и предотвратить возможные жертвы.

Немаловажную роль в пресечении преступлений в общественном транспорте играют такие системы как GPS, ГЛОНАСС и применение тахографического оборудования. С помощью данных систем возможно отслеживать маршруты общественного транспорта, контролировать

[1] Постановление Правительства РФ от 23.09.2017 № 1145 «О Межведомственной комиссии по внедрению и развитию систем аппаратно-программного комплекса технических средств «Безопасный город», системы обеспечения вызова экстренных оперативных служб по единому номеру "112" и Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС» // Собрание законодательства РФ, 02.10.2017, № 40, ст. 5850.

[2] Приговор Шадринского районного суда Курганской области от 20 июля 2021 г. № 1-295/2021 по делу № 1-295/2021 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/jW6qdZvy7nY4/.

поведение водителя автотранспорта, остановки и иные действия[1]. Помимо того, что с помощью данных систем обеспечивается безопасность как водителя общественного транспорта, так и пассажиров от возможных правонарушений с обеих сторон. Так и в случае совершения преступления или нарушения общественного порядка в транспорте, сотрудники правоохранительных органов могут получить достоверную значимую информацию из машинных данных без её искажения свидетелями. Так или иначе, как показывает практика, любая информация, которая поступает к человеку подвергается его психическому восприятию и искажается, приобретая субъективный характер.

Кроме того, на базе правоохранительных органов создаются специальные информационные центры, в архивах которых хранится вся информация о преступлениях, когда-либо зафиксированная компьютерными технологиями. Данная информация в последствии может использоваться сотрудниками правоохранительных органов для осуществления поисковых мероприятий или контроля за лицами, ранее совершившими преступления.

В настоящее время активно развивается создание алгоритмов машинного обучения – искусственного интеллекта.

Понятие искусственного интеллекта закреплено в Национальной стратегии развития искусственного интеллекта, под которым понимается «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное

[1] Федеральный закон от 28.12.2013 № 395-ФЗ (ред. от 30.12.2020) «О Государственной автоматизированной информационной системе «ЭРА-ГЛОНАСС» // Собрание законодательства РФ, 30.12.2013, № 52 (часть I), ст. 6960; Собрание законодательства РФ, 04.01.2021, № 1 (часть I), ст. 27.

обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений»[1].

Эффективность использования искусственного интеллекта при раскрытии и расследовании преступлений, а также при поиске необходимой доказательственной информации обусловлена его способностью имитировать когнитивные функции головного мозга человека. Алгоритм способен к самообучению и совершенствованию, он может находить и анализировать несравненно большие объемы информации гораздо быстрее и эффективнее, чем это может усвоить человеческий мозг при правильном вводе и описании признаков тех или иных предметов или явлений.

Искусственный интеллект может без участия человека использовать определенные математические модели и выявлять из толпы граждан на улице или на объектах транспортной инфраструктуры людей, которые могут совершать противоправные действия на основе их мимики, жестов и других признаков. Использование таких систем также позволит осуществлять поиск и задержание лиц, находящихся в розыске либо за совершение преступлений, либо пропавших без вести[2].

Используя системы на основе искусственного интеллекта, правоохранительные органы смогут прогнозировать совершение преступлений, выявлять наиболее опасные с точки зрения преступности места, патрулировать и контролировать их. Обеспечение безопасности общества является приоритетной задачей как государства в целом, так и правоохранительных органов в частности; построение правового общества и государства невозможно без борьбы с преступностью и неотвратимости наказания. А информационные технологии могут стать теми информационно-технологическими средствами, которые облегчат достижение задач расследования преступлений и станут теми

[1] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700.

[2] Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. №2 (104). С. 45.

инструментами, теми драйверами модернизации процессов предупреждения и борьбы с преступностью[1].

Так компьютерные программы, построенные на ИИ с глубоким обучением, способны на основе анализа определенных данных (данных с камер видеонаблюдения, данных о местонахождении и месте жительства преступников) уметь прогнозировать места преступлений. Однако еще раз отметим, что для этого требуется огромное количество данных, иначе это просто догадка. Анализируя прошлые преступления, можно предсказать возможность будущих преступлений, а также то, где и когда они могут произойти. Алгоритм такого прогноза помогает полиции повысить бдительность на соответствующих участках[2].

Развитие программ, прогнозирующих возможное время и место совершения преступления, следует рассматривать в контексте разработок по программе «Умный город», включая распознавание лиц (на улицах, вокзалах, аэропортах, транспорте и т.д.). При этом основным средством получения соответствующей информации являются камеры видеонаблюдения[3].

А учитывая, что некоторые из камер способны зафиксировать не только информацию о движении преступника по городу, но и его внешность (а при наличии камер, различающих биометрические параметры – личность), деятельность сотрудников правоохранительных органов становится в разы эффективнее.

Однако данные технологии имеются далеко не во всех городах России. В России в качестве «пилотного» проекта наиболее крупные объекты транспортной инфраструктуры (четыре региональных аэропорта, два морских порта, железнодорожный вокзал) были оснащены биометрическими камерами способными распознавать лица. Лица граждан сканировались

[1] Плахота К.С. К вопросу об использовании высоких технологий в расследовании преступлений // Расследование преступлений: проблемы и пути их решения. 2021. №3(33). С. 148.

[2] Степанян А.И. Предиктивная аналитика в прогностической деятельности полиции современных государств // Вестник Санкт-Петербургского университета МВД России. 2019. №4 (84). С. 45.

[3] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ, 31.08.2020, № 35, ст. 5593.

системой и сравнивались с лицами граждан, находящихся в розыске. При совпадении – сотрудникам, обеспечивающим безопасность, приходит оповещение[1].

Справедливо замечание И.В. Тишутиной, что у правоохранительных органов имеется множество информации: о преступлениях и преступниках, из различных баз данных (пулегильзотека, «Папилон»), однако вся собранная информация не оцифрована и не автоматизирована. Соответственно, на первое место выходит не объем данных, которыми располагают правоохранительные органы, а наличие в их распоряжении интеллектуальных платформ анализа и прогнозирования на основе больших данных[2].

В правоохранительных органах существует множество баз данных, однако информация, поступающая с камер видеонаблюдения, до сих пор не компонуется в специальной базе данных. Между тем, анализ видеозаписей позволил бы находить совпадения в поведении и внешнем облике лиц, что позволило бы раскрывать преступления «по горячим следам».

Также, в качестве одного из инструментов для предупреждения преступлений стоит рассмотреть социальные сети. В последнее время социальные сети все больше охватывают информационное пространство. По определению А. М. Лещенко «социальная сеть – симбиоз социальной и технической реальности, образовывающий многообразные коммуникативные конфигурации (пространственно-временные, субъект-субъектные, субъект-объектные), которые компенсируют высокую информационную плотность современного общества и осуществляют все виды социальной коммуникации

[1] Погодина И.В., Лазарева К.А. Организация контроля пассажиров в аэропортах Российской Федерации // Туризм: право и экономика. 2019. № 1. С. 27.

[2] Тишутина И.В. Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Известия ТулГУ. Экономические и юридические науки. 2019. №4. С. 49.

(массовой, межличностной, групповой) на всех технологических уровнях: вербальном, письменном, аудиовизуальном»[1].

Завоевывая аудиторию, социальные сети открывают широкие возможности для общения, получения новых знаний, воздействия на общество, широкие возможности для маркетологов и бизнеса. Немало трудов учёных разного уровня посвящено изучению социальных сетей с точки зрения предпосылок к совершению преступлений, а также их профилактики, особенно экстремистского и террористического характера.

Однако, несмотря на то, что органы государственной власти как на федеральном, так и региональном уровнях в настоящее время активно присутствуют в социальных медиа, вопрос взаимодействия полиции и общества на площадках в сети интернет практически не рассматривался с точки зрения научной и практической обоснованности[2].

По мнению Э.В. Намруевой цель, к которой стремится МВД России – это высокий уровень доверия граждан «…достижение этой цели возможно лишь на основе использования новых форм взаимодействия полиции и общества»[3].

К таким новым формам и относится развивающийся институт социальных медиа. Эффективное взаимодействие предполагает обратную связь, возможность обмениваться информацией друг с другом. Размещение в социальных сетях только информационного контента не обеспечивает в полной мере диалога граждан и полиции, за исключением комментариев к постам, однако они в большинстве своем не несут полезной информационной нагрузки для органов внутренних дел.

---

[1] Лещенко А.М. Мультифункциональность сетевых коммуникаций в современном обществе // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2011. №2. С. 130.

[2] Валединская Е. Н., Астафьева О. А., Бочарова Э. А. Специфика эффективного маркетинга в социальных сетях // Дискуссия. 2017. № 3. С. 25.

[3] Намруева Э. В. Использование социальных сетей в деятельности подразделений информации и общественных связей органов внутренних дел: отечественный и зарубежный опыт // Вестник Московского университета МВД России. 2018. № 3. С. 36.

Например, сотрудники уголовного розыска и следователи Управления министерства внутренних дел Российской Федерации по Забайкальскому краю (далее – УМВД России по Забайкальскому краю) все чаще стали прибегать к потенциалу социальных сетей при раскрытии и расследовании преступлений, поиску очевидцев, свидетелей, а зачастую и подозреваемых, путем размещения фото и видео с мест совершения преступлений.

Анализ практики раскрытия преступлений говорит о том, что портретная экспертиза имеет важное, а нередко и определяющее значение при расследовании уголовных дел. Являясь так называемой «традиционной криминалистической экспертизой», наряду с другими видами, портретная экспертиза проводится с целью идентификации человека по признакам внешности, отобразившимся на фотографиях и других носителях изображений. В последнее время в оперативных и следственных подразделениях органов внутренних дел значительное развитие получила криминалистическая идентификация человека по видеозаписям[1].

Все чаще в качестве объектов стали выступать видеоизображения, полученные с уличных камер видеонаблюдения или установленных в магазинах, банках, развлекательных заведениях. Повсеместное использование камер видеонаблюдения значительно облегчает процесс опознания лиц, участвовавших в совершении преступления и установления обстоятельств его совершения, однако нередко отождествить оперативным путем лицо, которое запечатлено на видео, не представляется возможным. Здесь на помощь приходит общественность, обратиться к которой можно посредством СМИ и сети Интернет. В данном случае не лишним будет сказать, что традиционные СМИ (телевидение, газеты, радио) уже не пользуются такой популярностью в качестве источника получения информации, уступив место интернет-порталам и социальным сетям.

[1] Михайлова М.С. Отдельные вопросы проведения портретной экспертизы в рамках криминалистического исследования // Международный журнал гуманитарных и естественных наук. 2019. №11-3. С. 38.

Однако здесь стоит оговориться и отметить, что для получения конечного результата в виде раскрытия преступления важно установить обратную связь непосредственно с оперативным сотрудником или следователем, указав в ориентировке контактный телефон исполнителя, а не дежурной части территориального органа или 02. Не каждый сознательный гражданин, имеющий желание оказать содействие органам внутренних дел, будет набирать несколько номеров и пытаться дозвониться. Гораздо проще сообщить информацию в личном сообщении (ВКонтакте, Одноклассники) или в директ (Инстаграм).

Так, 26 декабря 2018 года по рапорту сотрудников уголовного розыска на страницах социальных сетей УМВД России по Забайкальскому краю была размещена видеоориентировка на подозреваемого в краже куртки у посетителя развлекательного заведения. В этот же день в директ УМВД поступило сообщение от подписчика, который сообщил, что гражданин, изображенный на видео, внешне схож с молодым человеком, работающим на одной из автомоек Читы, указав адрес этой организации. Полученная информация была передана сотрудникам уголовного розыска. В результате лицо, совершившее кражу, было задержано и преступление раскрыто.

Таким образом, современные информационные технологии, выполняя коммуникативную функцию, могут быть полезны не только различным категориям граждан, позволяя общаться, но и органам государственной власти, помогая выполнять возложенные задачи, в том числе по борьбе с преступностью.

2.2. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационных технологий

В современном мире информационные технологии служат не только инструментом эффективной борьбы с преступностью, но и нередко являются средством совершения преступлений. Исходя из этого, представляется целесообразным в рамках данной выпускной квалификационной работы

рассмотреть основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационных технологий.

Исходя из статистических данных МВД России, с каждым годом в нашей стране возрастает количество киберпреступлений[1]. Об этом же свидетельствуют и данные, представленные Банком России. Так, за 2019 г. им было заблокировано более 13 тыс. телефонных номеров, которые использовались в мошеннических целях, что в 29 раз больше, чем в 2018 г.; ограничены 1107 ресурсов, распространяющих вредоносное программное обеспечение, 10 683 фишинговых ресурсов (их стало в пять раз больше), 370 массовых фишинговых рассылок. Информация о более чем 250 доменах в целях ограничения доступа направлена в Генеральную прокуратуру Российской Федерации[2].

Особенной популярностью у преступников сегодня пользуются сервисы IP-телефонии, с помощью которых можно беспрепятственно и без прохождения процесса идентификации подключаться к стационарным телефонам. Применяя такие сервисы, можно осуществлять звонки как с помощью компьютера, посредством установки на компьютер специальной программы, с помощью планшетного компьютера, мобильного или стационарного телефона.

Подобную технологию применяют в своей работе колл-центры, поскольку им необходимо с разных средств связи одновременно звонить разным людям, но с одного и того же номера телефона – указанного на сайте организации. Мошенники действуют по такому же принципу. Это позволяет им звонить в любой регион страны, за относительно недорогую стоимость и идентифицировать данный звонок не представляется возможным.

Также, в практике нередки случаи, когда мошенники звонят жертвам с имитацией реальных номеров службы поддержки банка. На сегодняшний

[1] Официальный интернет-сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

[2] Официальный сайт Центрального Банка Российской Федерации [Электронный ресурс]. – Режим доступа: https://cbr.ru/.

день такая ситуация стала возможной, поскольку в сети Интернет содержится большое количество уязвимых для взлома автоматических телефонных станций. Злоумышленники взламывают эти станции и используют полученные данные, а именно – номера телефонов в криминальных целях.

Например, в 2020 г. житель города Красноярска О. решил с помощью информационно-телекоммуникационных сетей совершить хищение денежных средств. С этой целью О. в Интернете приобрёл специальную программу, с помощью которой возможно обеспечить цифровое голосовое общение удаленных абонентов в целях передачи голоса IP-сетью посредством подменного абонентского номера. С помощью данной программы О. совершил звонок гражданину П. в Калмыкию и представившись сотрудником ПАО «Сбербанк России» обманом узнал у гражданина П. все необходимые коды, позволяющие управлять денежными средствами, находящимися на его счетах через мобильное приложение. Таким образом, О. похитил у гражданина П. определённую сумму денежных средств и распорядился ими по собственному усмотрению[1].

Ещё одной значимой проблемой при раскрытии преступлений, совершаемых с использованием информационных технологий, является использование злоумышленниками средств, создающих препятствие для идентификации. Одним из таких популярных и широко применяемых средств служит VPN (англ. Virtual Private Network – виртуальная частная сеть). Использование данной программы позволяет пользователям полностью скрыть или значительно затруднить процесс получения данных об их местоположении. В настоящее время использование VPN в России является легальным и никак не регулируется законодательством[2].

[1] Приговор Малодербетовского районного суда республики Калмыкии от 28 марта 2022 г. по делу №1-4 (2022) (1-77/2021) // Официальный сайт Малодербетовского районного суда Республики Калмыкия [Электронный ресурс]. Режим доступа – http://maloderbetovsky.kalm.sudrf.ru/.

[2] Костенко Н.С., Семененко Г.М., Пшеничкин А.А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе // Вестник ВИ МВД России. 2020. №4. С. 194.

Также, не урегулирована деятельность по производству, реализации и использованию программных и программно технических автоматических телефонных станций IP-телефонии. Помимо этого, цена данной услуги незначительна, что позволяет свободно размещать телефонные серверы практически во всех странах.

Кроме того, сложность в раскрытии и расследовании преступлений, совершаемых с использованием информационных технологий, обуславливается тем, что преступники практически никогда не совершают преступления в том регионе, в котором они сами находятся. С целью ввести в заблуждение следствие, а также скрыть следы своих преступлений, чаще всего злоумышленники используют сим-карты и банковские счета, зарегистрированные на подставных лиц. Также, нередки случаи, когда злоумышленники используют виртуальные платежные системы, и карты банков зарубежных государств, которые не выдают России сведения об их владельцах[1].

Проанализировав следственно-судебную практику относительно преступлений, совершённых с использованием современных информационных технологий, удалось выявить следующие, наиболее распространённые преступления:

– мошенничество путем направления СМС-сообщения – мошенники направляют СМС-сообщения о проведении транзакций по счету потерпевшего (списание денежных средств со счета или блокировка карты), после чего просят потерпевшего сообщить реквизиты и пароли доступа к операциям по счету посредством поступившего им СМС-сообщения, что приводит к хищению денежных средств.

Например, М. отбывала наказание в одной из колоний Пермского края за 11 краж, несколько эпизодов мошенничества и других преступлений. Следствие обвинило М. в том, что в период отбывания наказания она,

[1] Великородный П.Г. Сокрытие следов преступления и противодействие его расследованию как способ уклонения от уголовной ответственности // Вестник СГЮА. 2018. №2 (121). С. 183.

используя телефон, совершила 37 эпизодов мошенничества. Вместе с неустановленным следствием лицом она рассылала СМС-сообщения о блокировании банковских карт потерпевших. Потерпевшие перезванивали М., которая выдавала себя за работника банка. В телефонном разговоре она под предлогом обеспечения сохранности денег потерпевшего убеждала перевести деньги на подконтрольные ей счета[1].

– мошенничество с предоплатой – обман при осуществлении купли-продажи товаров на соответствующих интернет-сайтах (Avito.ru, «Юла», «Флагма» и др.).

– взлом аккаунта в социальных сетях с последующей рассылкой сообщений в адрес друзей и знакомых с просьбой перевести денежные средства – мошенники, пользуясь беспечностью граждан, путем использования специального программного обеспечения получают доступ к страницам пользователей социальных сетей, после чего от имени пользователя запускают рассылку сообщений всем контактам «взломанной страницы» с просьбой оказать материальную помощь в сложной жизненной ситуации или дать в долг;

– участие в интернет-опросах или сообщение о выигрыше в лотерею, получение компенсации за оказанные ранее услуги и т.д. – мошенники предлагают пользователям сети Интернет крупную сумму денег за участие в интернет-опросе либо сообщают гражданам о крупном выигрыше в лотерею. При этом просят произвести «закрепительный платеж», необходимый для оформления соответствующих документов либо уплаты налогов;

– совершение звонков под видом работников социальных органов с информацией о полагающейся компенсации за ранее приобретенные

[1] Решение Октябрьского районного суда г. Тамбова № 12-524/2017 от 28 сентября 2017 г. по делу № 12-524/2017 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/nyHN1d6cw7ri/.

лечебные аппараты, медикаменты, БАДы и т.д. После перевода потерпевшим платежа дальнейшее общение с ним прекращается;

– использование дубликата сим-карты для доступа к системам дистанционного управления банковским счетом. Признаком использования дубликата сим-карты абонента является блокирование доступа мобильной связи;

– совершение звонков в службы доставки с последующей просьбой пополнить баланс счета сотового телефона и т.д.

– преступлений, которые квалифицируются как мошенничество, совершаемые с использованием банковских карт в информационном пространстве. По данным компании Sift, разработчика инструментов для реагирования на киберинциденты, показатели атак, связанных с покушением на мошенничество с платежами, возросло на 70%, что является высоким показателем. За прошедший год убытки клиентов российских банков из-за мошеннических схем достигли 3,15 млрд. рублей, причем, исходя из отчета, потерпевшие лица в течение 2021 года совершали 11776 переводов ежедневно, что суммарно составило 8,16 млн. рублей в день.

Наиболее частым при расследовании преступлений данной категории встает вопрос определения места совершения преступления, так как в сегодняшних реалиях буквально каждый потенциальный субъект уголовных правоотношений с легкостью может перемещаться по различным территориям и при этом менять геолокацию на телефоне или ином средстве, на котором у лица есть доступ к сети Интернет. Очевидным становится вопрос верного определения места производства предварительного расследования такого вида неправомерных действий. Так же ключевой является проблема необоснованного искусственного ограничения круга вопросов о месте рассмотрения сообщения о таких преступлениях.

Вышеуказанные проблемы возникают у правоприменителей при возбуждении уголовных дел. Они прямо указывают на то, что такие преступные деяния могут совершаться и без фактического контакта с

потерпевшим, а в некоторых случаях, и вовсе без их реального участия. Некоторые ученые, к примеру, А.А. Лаврушкина, в своих исследованиях указывают на момент трансграничности мошеннических действий и иных преступных действий в данной области, что особенно актуально при квалификации такого рода деяний[1].

Таким образом, обращаясь к сущности рассматриваемой нами темы, неверное определение территориальной подследственности приводит к многократному и необоснованному направлению сообщений о преступлениях, что в свою очередь, является порождающим фактором для момента несоблюдения процессуальных и иных сроков уголовного судопроизводства, которые важно учитывать. В науке существует несколько точек зрения по поводу определения места совершения данного рода преступлений.

Некоторые авторы, склоняются к тому, что местом окончания преступления с использованием счетов интернет-банка будет то место, из которого отправлены денежных средства потерпевшим. Ученые связывают данную позицию с тем, что именно в тот момент наступают последствия для субъекта, который совершил операцию. Другие авторы придерживаются позиции, суть которой заключается в определении места совершения данного преступления согласно принципу целесообразности. Она состоит в том, что расследовать такое уголовное дело необходимо в том районе, в котором оно было совершено, то есть именно там, где были обнаружены следы преступления.

Также существует мнение, что при определении места предварительного расследования следует обращаться к статье 152 Уголовно-процессуального кодекса Российской Федерации[2], суть которой заключается в указывании на трансграничность и момент того, что в каждом конкретном

[1] Лаврушкина А.А. Типичные следственные действия в рамках методики расследования мошенничества с использованием сети Интернет и средств мобильной связи // Бюллетень науки и практики. 2018. №4. [Электронный ресурс] Режим доступа: URL:https://cyberleninka.ru/article/n/tipichnye-sledstven.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 07.10.2022) // Собрание законодательства Российской Федерации. 2001. № 52 (I часть). Ст.4921.

случае при заявлении лица следует учитывать специфику неправомерности списания денежных средств с банковской карты.

Так, А.В. Маилян прямо указывает на важность срочного рассмотрения такого рода заявлений и своевременность исследования всех вопросов, которые связаны с сущностью их совершения. Здесь следует направить дело по подследственности в порядке статьи 152 УПК РФ, если при установлении в ходе производства предварительного расследования точного места совершения преступления, возник вопрос о подведомственной территории[1].

Некоторые ученые предполагают, что местом совершения преступления будет место нахождения преступника. Важным становится вопрос о квалификации всех действий лица, совершившего незаконную транзакцию. Следует рассматривать вопрос о поэтапных действиях такого субъекта. В данном вопросе следует вспомнить, что орган дознания, следователь, дознаватель обязаны своевременно зафиксировать факт обращения к ним лица, сообщающего о преступном деянии в банковской области в процессе перевода денежных средств с одного счета на другой незаконными путями без согласия потерпевшей стороны[2]. Таким образом, мы можем сделать вывод о том, что точек зрения по поводу определения подследственности достаточно много. Так, к примеру, стоит рассматривать случаи, когда лицо получило деньги путем обмана.

В Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[3] отмечается, что преступление окончено не там, где лицо совершило перевод, а там, где был открыт банковский счет, но, если говорить о части,

[1] Маилян А.В. Особенности возбуждения уголовного дела о хищении,совершенном с использованием электронных средств платежа // Вестник Сибирского юридического института МВД России. 2021. №2 (43). С. 35.

[2] Степанова М.А., Царёв Е.В. Проблемы определения места совершения хищения денежных средств с использованием информационнотелекоммуникационных технологий // Вестник БелЮИ МВД России. 2021. №1. С. 14.

[3] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] Режим доступа: http://www.consultant.ru/.

применительно к нашему случаю, то это те места, где лицо получило денежные средства по переводу. Как следствие, фактическое место нахождения преступника. Обратимся к родовой подследственности. Хочется особенно заметить, что существующая классификация по предмету подследственности ставит перед органами следствия вопросы о более тщательном прорабатывании момента квалификации совершенного деяния и последующего более эффективного процесса расследования. Родовой подследственностью считается та, что происходит исходя из состава расследуемого преступления, выраженного в его квалификации. Так, важным становится вопрос об определении конкретного органа, расследующего совершенное деяния, а также, формы предварительного расследования, то есть, следствия или дознания.

Исходя из всего вышесказанного, мы можем сделать вывод о том, что в целях соблюдения целей уголовного судопроизводства стоит брать в расчет момент рассмотрения принципов, на основе которых ведется расследование преступлений, как следствие, говоря о месте окончания преступлений, связанных с переводом денежных средств на счета интернет-банков, таковым будет в большинстве случаев считаться место перечисления денежных средств, притом, нельзя исключать возможность принятия во внимание место обращения потерпевшего в полицию.

Таким образом, в аспекте повышения эффективности расследования указанных преступлений необходимо:

– проработать вопрос о заключении обязательных соглашений с банками, коммерческими организациями, предоставляющими услуги IP-телефонии, платежными системами, социальными сетями, операторами сотовой связи, провайдерами сети Интернет на предмет осуществления электронного документооборота с подразделениями МВД по направлению запросов и получению ответов в электронном виде посредством ведомственного сервиса электронного документооборота (СЭД);

– рассмотреть вопрос о внесении изменений в статью 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»[1] в части выдачи справок по операциям и счетам юридических лиц, граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также физических лиц не только органам предварительного следствия по делам, находящимся в их производстве, но и органам дознания;

– проработать вопрос с ФСИН России о создании и ведении фоноскопического учета лиц, отбывающих (отбывавших) наказание в местах лишения свободы;

– проработать вопрос с кредитно-финансовыми учреждениями об увеличении сроков хранения видеоизображений с банкоматов и из операционных залов;

– рассмотреть вопрос о введении специализации следователей по расследованию преступлений данной категории.

Перечень обозначенных нами вопросов в рамках раскрытия и расследования преступлений, совершаемых с использованием инновационных технологий, конечно же, не является исчерпывающим. Однако рассмотренный нами комплекс обстоятельств, способствующих совершению указанных преступлений, а также предложенные меры по раскрытию и расследованию данных преступлений помогут совершенствовать общественные отношения в данной области и снизить число таких преступлений на территории Российской Федерации.

[1] Федеральный закон от 02.12.1990 № 395-1 (ред. от 14.07.2022) «О банках и банковской деятельности» // Собрание законодательства РФ, 05.02.1996, № 6, ст. 492; Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5259.

2.3. Пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений

В нынешних обстоятельствах «цифровой революции» непосредственные информационные процессы становятся основным условием изменения, а также оптимизации работы каждого государственного органа и МВД РФ тут никак не редкий случай.

Исходя из проведённого исследования, считаем целесообразным выделить некоторые пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений.

Изучение следственно-судебной практики позволил выявить некоторые проблемы, возникающие при расследовании преступлений в сфере информационных технологий, а именно:

1) Длительность (до нескольких месяцев) получения информации, имеющей доказательственное значение по уголовным делам от компаний операторов сотовой связи и финансово-кредитных учреждений (сведений о владельцах сим-карт и банковских карт, движении денежных средств потерпевшего и подозреваемого и др.).

Для решения данной проблемы правоохранительным органам и организациям – обладателям информации, целесообразно организовывать электронный обмен документами и соответствующими сведениями на основе действующего законодательства и заключённых договоров о сотрудничестве.

2) Использование для совершения преступлений сим-карт и банковских карт, оформленных на других лиц, а также смена преступниками мобильных телефонов и абонентских номеров сим-карт.

Решение этой проблемы видится в усилении контроля за деятельностью операторов связи по распространению сим-карт. Эффективность подобного контроля возросла с 1 июня 2018 г., когда вступил в силу Федеральный закон от 29 июля 2017 г. № 245-ФЗ «О внесении

изменений в Федеральный закон «О связи» в соответствии с которым «…лицо, действующее от имени оператора связи, при заключении договора об оказании услуг подвижной радиотелефонной связи обязано внести в него достоверные (выделено авт.) сведения об абоненте…»[1].

Также, оператор связи обязан осуществлять проверку достоверности сведений об абоненте и сведений о пользователях услугами связи абонента – юридического лица либо индивидуального предпринимателя, в том числе представленных лицом, действующим от имени оператора связи, в соответствии с настоящим Федеральным законом и правилами оказания услуг связи.

3) Недостаточное количество экспертов, имеющих допуск к производству компьютерно-технических судебных экспертиз, значительная длительность их производства, существенная стоимость при проведении в иных учреждениях (до нескольких сотен тысяч рублей за одну экспертизу).

Решить вопрос с подготовкой экспертов необходимого профиля поможет только ориентация ВУЗов на данную деятельность.

В контексте рассматриваемого вопроса следует отметить, что исполнение требований закона (ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ) об обязательном участии специалиста при изъятии электронных носителей информации отвлекает экспертов от выполнения экспертиз, что влечет увеличение срока расследования.

Одним из способов решения подобной проблемы, может быть привлечение к участию в процессуальных действиях сотрудников не государственных организаций, специализирующихся на информационной безопасности.

В качестве положительного примера можно привести успешное расследование преступления, возбужденного 25 декабря 2015 г. СУ УМВД России по г. С. по признакам преступления, предусмотренного ч. 1 ст. 272

[1] Федеральный закон от 29.07.2017 № 245-ФЗ (ред. от 05.12.2017) «О внесении изменений в Федеральный закон «О связи» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4794.

УК РФ в отношении И. и направление материалов в суд, чему способствовало привлечение специалистов местного Интернет-провайдера, которые оказали помощь в установлении IP-адреса и места, с которого обвиняемый, путем подбора пароля, осуществил несанкционированный доступ и временно заблокировал электронный почтовый ящик С[1].

6) Недостаточные сроки хранения электронной информации в финансово-кредитных учреждениях, у операторов платежных систем и операторов сотовой связи.

Решение данной проблемы видится в реализации положений ст. 64 Федерального закона от 7 июля 2003 г.№ 126-ФЗ «О связи», в соответствии с которыми операторы связи обязаны хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий, а текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки[2].

В этом же законе зафиксировано, что операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач.

---

[1] Решение Ярославского областного суда от 6 июля 2021 г. № 3А-451/2021 3А-451/2021~М-268/2021 М-268/2021 по делу № 3А-451/2021 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/jW6qdZvy7nY4/.

[2] Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 30.12.2021) «О связи» (с изм. и доп., вступ. в силу с 01.05.2022) // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895; Собрание законодательства РФ, 03.01.2022, № 1 (Часть I), ст. 34.

7) отсутствие единого подхода в различных субъектах Российской Федерации к квалификации однотипных преступлений данной категории.

Решение данной проблемы видится в принятии Постановления Пленума Верховного Суда Российской Федерации по делам о преступлениях в сфере информационных технологий, подготовке и распространению разъяснений Генеральной Прокуратурой Российской Федерации совместно с правоохранительными органами, обеспечивающими расследование подобных преступлений.

8) стоит также обратить внимание на невозможность или сложность получения экстерриториальных данных, информации, хранящейся на серверах иностранных государств и находящейся вне юрисдикции следственных органов. Особенно данный фактор осложнился из-за специальной военной операции на Украине и введению против России санкций большинства государств мира.

В этих целях целесообразно налаживать связь с поставщиками услуг и разработчиками информационных систем, обладающими правами использования, хранения и обработки данных о пользователях, в том числе о совершаемых ими действиях. Встречаются случаи, когда невозможность причисления отдельных форм преступлений в цифровом пространстве к существующим правовым нормам весьма затрудняет и затягивает ход расследуемого дела. Так, невзирая на наличие общезаконодательных мер, отсутствуют положения, рассматривающие подкатегории киберпреступлений в отдельности, по степени нанесения вреда и пр., в связи с этим намечается необходимость проведения мониторинга совершаемых киберпреступлений с целью выработки объективных законодательных мер[1].

В настоящее время в России наблюдается неудовлетворительный уровень технического оснащения подразделений, специализирующихся на расследовании киберпреступлений. Необходимо констатировать

[1] Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений // Вестник БелЮИ МВД России. 2020. №3. С. 21.

существенный дефицит таких элементарных технических средств, как средства выемки аппаратного обеспечения и электронных доказательств; средства моделирования электронных образов и хэш-кодов, восстановления данных по «отпечаткам» в памяти жестких дисков, обработки и расшифровки данных; средства дистанционной экспертизы оборудования и ликвидации информации.

Очевидно, что приоритетным направлением финансирования кибербезопасности и основополагающим фактором её достижения является качественное техническое оснащение. Киберпреступники систематически совершенствуют инструменты киберпреступлений, что позволяет им всегда находиться на шаг впереди правоохранительных органов. Необходимо осознавать, что обе противоборствующие стороны обладают одним инструментом борьбы, т.е. фундаментальным условием результативности работы правоохранительных органов здесь служат инновации, их активное внедрение и использование.

9) особое внимание стоит уделять подготовке специализированных кадров. Сейчас в стране неудовлетворительный уровень подготовки следователей, привлекаемых к расследованию и раскрытию киберпреступлений. Данное обстоятельство в первую очередь объясняется отсутствием традиции обучения юристов высокотехнологичным дисциплинам, отставанием более консервативной юриспруденции от стремительно развивающейся инженерии. Также недостаточный уровень квалификации сотрудников, привлекаемых к раскрытию преступлений в области информационных технологий, обусловлен цифровой революцией[1]. Часто обучение специалистов осуществляется с большим временным отрывом, что особенно заметно в данной области в условиях глобализации. Центральной проблемой, препятствующей качественной подготовке киберследователей в борьбе с киберкриминалом, является дефицит

[1] Харисова З.И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник УЮИ. 2019. №3 (85). С. 95.

практического опыта по расследованию киберпреступлений у преподавателей. Даже лучшие «старые» кадры, результаты деятельности которых характеризуются феноменальной раскрываемостью, не располагают достаточными знаниями об инновационных методиках преступлений в интернет-пространстве, специфичных в своей динамичности и технической сложности совершения. Одновременно с этим представители поколения Z («цифровые аборигены»), обучающиеся сегодня в образовательных организациях системы МВД России и обладающие высоким уровнем знаний и компетенций в данных областях, не имеют необходимой процессуальной подготовки и опыта следственной работы.

По мнению экспертов, в настоящий период существует целый комплекс проблем в рамках подготовки специалистов по раскрытию и расследованию преступлений вузами МВД России:

1. Программы повышения квалификации в образовательных организациях системы МВД России по линии расследования киберпреступлений носят исключительно теоретический характер, практические занятия отсутствуют.

2. Повышение квалификации профессорско-преподавательского состава и специалистов в области киберпреступлений в сторонних организациях требует огромных финансовых издержек – стоимость обучения в данных организациях составляет более 300 000 рублей.

3. Неудовлетворительный уровень заработной платы сотрудников правоохранительных органов. Данное обстоятельство служит серьезным демотивирующим фактором для выпускников технических вузов и специалистов в сфере высоких технологий в поступлении на службу в ОВД. Если в зарубежных странах расследованием киберпреступлений занимаются главным образом специалисты с высшим техническим образованием и дополнительным юридическим, то в России данный сценарий нереалистичен.

Кроме того, небольшой процент выпускников технических вузов, который все же поступает на службу в ОВД, как правило, направляется в

дальнейшем не в Управление «К» или иные службы, задействованные в раскрытии и расследовании киберпреступлений, а в подразделения полиции общественной безопасности или тыловые подразделения. Таким образом, осуществляется крайне нерациональное использование человеческого капитала.

В заключении следует отметить, что решение основных проблем возникающих при расследовании преступлений в сфере информационных технологий возможно только при комплексном взаимодействии государственных органов и представителей бизнеса, специализирующихся на вопросах информационной безопасности. Необходимость привлечения таких специалистов для противодействия киберпреступности и в целях обеспечении безопасности киберпространства обусловлена децентрализованной структурой современных информационно-телекоммуникационных сетей и их трансграничным характером. Только обеспечив подобное взаимодействие появится возможность успешно расследовать преступления в сфере информационных технологий, обеспечить информационную безопасность и технологическую независимость России на должном уровне.

Вывод по главе:

В современном мире применение современных информационных технологий для предупреждения и пресечения преступлений является одной из самых приоритетных задач для государства. В настоящее время создаются центры обработки и хранения информации, которые позволяют выявлять и пресекать преступления. Внедряются системы видеофиксации в общественных местах, что позволяет значительно снизить число преступлений против имущества граждан и оперативно выявлять и пресекать нарушения общественного порядка. Немаловажную роль в пресечении преступлений в общественном транспорте играют системы GPS, ГЛОНАСС и применение тахографического оборудования, что позволяет планировать маршруты движения автотранспорта, контролировать поведения водителя

при движении по маршруту, остановки и иные действия. Также, сейчас идёт активная разработка искусственного интеллекта, что позволит в дальнейшем вывести практику борьбы с преступностью и поиско-познавательную деятельность правоохранительных органов государства на новый технологический уровень.

Анализируя основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационных технологий удалось выявить следующие:

1) существует препятствие для идентификации мошенников, поскольку злоумышленники при совершении преступных деяний прибегают к использованию различных программных средств, позволяющих шифровать свои данные;

2) в настоящий момент производство, реализация и использование программных и программно-технических АТС IP-телефонии практически никак не регулируется государством, что создаёт проблемы и практически исключает возможность привлечения к ответственности, в случае противоправных действий в этой области;

3) также существует проблема нежелания некоторых коммерческих структур, действующих на территории Российской Федерации, сообщать в правоохранительные органы о совершении противоправных действий как в отношении самих компаний и их клиентов, так и компаний, которым стала известна информация о совершаемых или готовящихся преступлениях посредством связи с использованием зашифрованных программ;

4) наиболее частым при расследовании преступлений, с использованием средств сотовой связи встает вопрос определения места совершения преступления, так как в сегодняшних реалиях буквально каждый потенциальный субъект уголовных правоотношений с легкостью может перемещаться по различным территориям и при этом менять геолокацию на телефоне или ином средстве, на котором у лица есть доступ к сети Интернет. Очевидным становится вопрос верного определения места производства

предварительного расследования такого вида неправомерных действий. Так же ключевой является проблема необоснованного искусственного ограничения круга вопросов о месте рассмотрения сообщения о таких преступлениях.

По результатам проведённого исследования, были предложены следующие пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений:

1) правоохранительным органам и организациям – обладателям информации, целесообразно организовывать электронный обмен документами и соответствующими сведениями на основе действующего законодательства и заключённых договоров о сотрудничестве;

2) для предотвращения использования сим-карт и банковских карт, оформленных на других лиц, а также смены преступниками мобильных телефонов и абонентских номеров сим-карт для совершения преступлений предлагает усилить контроль за деятельностью операторов связи по распространению сим-карт;

3) представляется целесообразным закрепить в законодательстве право привлекать к участию в процессуальных действиях при проведении изъятия электронных носителей информации сотрудников не государственных организаций, специализирующихся на информационной безопасности, что позволит не отвлекать экспертов от выполнения компьютерно-технических судебных экспертиз;

4) в настоящее время в субъектах Российской Федерации нет единого подхода в отношении квалификации однотипных преступлений в сфере информационных технологий, что приводит к противоречиям правоприменительной практики. Исходя из этого, существует объективная необходимость в принятии Постановления Пленума Верховного Суда Российской Федерации по делам о преступлениях в сфере информационных технологий.

ЗАКЛЮЧЕНИЕ

На основе проведённого в выпускной квалификационной работе исследования были сделаны следующие выводы.

1. Исследуя теоретические основы использования информационного обеспечения и информационных технологий в раскрытии и расследовании преступлений, удалось сформировать такие понятия как «информационные технологии» и «информационное обеспечение».

Так, под информационными технологиями в действующем законодательстве Российской Федерации понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Данное определение закреплено в Федеральном законе «Об информации, информационных технологиях и о защите информации».

Понятие «информационное обеспечение» в современном российском законодательстве не закреплено. Нет единого подхода к трактовке данного термина и среди учёных. Одни учёные считают, что при определении понятия «информационное обеспечение» следует применять технические термины, по мнению других в содержании понятия «информационное обеспечение» должно содержаться решение задач оперативно-розыскной деятельности.

На наш взгляд, при определении информационного обеспечения предварительного расследования стоит говорить о конкретном наборе инструкций и данных, позволяющих решать такие вопросы как: выбор субъектов сбора информации, их компетенции; определение сроков, порядка и способов получения, фиксации, обработки и систематизации получаемой информации; анализ информации в рамках определенной процедуры с применением типовых методик и привлечением соответствующих специалистов; организация использования результатов анализа информации в практической деятельности органов предварительного следствия.

2. Рассматривая информационные технологии, которые в настоящее время применяются сотрудниками правоохранительных органов при раскрытии и расследовании преступлений, удалось выявить следующие:

5) Справочно-правовая информационная система (СПИС);
6) Программный комплекс «Гранд УД»;
7) Дактилоскопическая идентификационная система «АДИС»;
8) Автоматизированная система «Квадрат».

Нами были рассмотрены самые эффективные и широко применяемые правоохранительными органами инновационные средства для раскрытия и расследования преступлений, однако это далеко не все. В современном мире рименение информационных технологий в раскрытии и расследовании преступлений приобретает всё большую актуальность в условиях модернизации всех сфер современной жизни. Использование современных технологий способствует оптимизации и повышению эффективности работы правоохранительных органов в раскрытии и расследовании преступлений.

3. Определяя перспективы использования новых информационных технологий в раскрытии и расследовании преступлений удалось прийти к выводу о том, что на сегодняшний день самым перспективным является внедрение технологий «искусственного интеллекта». Благодаря этому, в будущем есть возможность повышения эффективности раскрытия преступлений. Данное внедрение в практику также должно быть направлено на защиту граждан от преступных посягательств. Помимо этого, сейчас в системе Министерства внутренних дел Российской Федерации совершенствуется режим ЭВМ, который обеспечивает быстрое выполнение задач оперативно-розыскного и учетно-статистического характера. Реализация намеченных планов позволит нашей стране выйти в первые ряды лидеров российской науки, а также МВД предполагает тем самым повысить раскрываемость преступлений и правонарушений.

4. В современном мире использование современных информационных технологий для предупреждения и пресечения преступлений является одной

из самых приоритетных задач для государства. В настоящее время создаются центры обработки и хранения информации, которые позволяют выявлять и пресекать преступления. Внедряются системы видеофиксации в общественных местах, что позволяет значительно снизить число преступлений против имущества граждан и оперативно выявлять и пресекать нарушения общественного порядка. Немаловажную роль в пресечении преступлений в общественном транспорте играют системы GPS, ГЛОНАСС и применение тахографического оборудования, что позволяет планировать маршруты движения автотранспорта, контролировать поведения водителя при движении по маршруту, остановки и иные действия. Также, сейчас идёт активная разработка искусственного интеллекта, что позволит в дальнейшем вывести практику борьбы с преступностью и поиско-познавательную деятельность правоохранительных органов государства на новый технологический уровень.

5. Анализируя основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационных технологий удалось выявить следующие:

1) существует препятствие для идентификации мошенников, поскольку злоумышленники при совершении преступных деяний прибегают к использованию различных программных средств, позволяющих шифровать свои данные;

2) в настоящий момент производство, реализация и использование программных и программно-технических АТС IP-телефонии практически никак не регулируется государством, что создаёт проблемы и практически исключает возможность привлечения к ответственности, в случае противоправных действий в этой области;

3) также существует проблема нежелания некоторых коммерческих структур, действующих на территории Российской Федерации, сообщать в правоохранительные органы о совершении противоправных действий как в отношении самих компаний и их клиентов, так и компаний, которым стала

известна информация о совершаемых или готовящихся преступлениях посредством связи с использованием зашифрованных программ;

4) наиболее частым при расследовании преступлений, с использованием средств сотовой связи встает вопрос определения места совершения преступления, так как в сегодняшних реалиях буквально каждый потенциальный субъект уголовных правоотношений с легкостью может перемещаться по различным территориям и при этом менять геолокацию на телефоне или ином средстве, на котором у лица есть доступ к сети Интернет. Очевидным становится вопрос верного определения места производства предварительного расследования такого вида неправомерных действий. Так же ключевой является проблема необоснованного искусственного ограничения круга вопросов о месте рассмотрения сообщения о таких преступлениях.

6. По результатам проведённого исследования, были предложены следующие пути совершенствования мер и возможностей использования современных информационных технологий в раскрытии и расследовании преступлений:

1) правоохранительным органам и организациям – обладателям информации, целесообразно организовывать электронный обмен документами и соответствующими сведениями на основе действующего законодательства и заключённых договоров о сотрудничестве;

2) для предотвращения использования сим-карт и банковских карт, оформленных на других лиц, а также смены преступниками мобильных телефонов и абонентских номеров сим-карт для совершения преступлений предлагает усилить контроль за деятельностью операторов связи по распространению сим-карт;

3) представляется целесообразным закрепить в законодательстве право привлекать к участию в процессуальных действиях при проведении изъятия электронных носителей информации сотрудников не государственных организаций, специализирующихся на информационной безопасности, что

позволит не отвлекать экспертов от выполнения компьютерно-технических судебных экспертиз;

4) в настоящее время в субъектах Российской Федерации нет единого подхода в отношении квалификации однотипных преступлений в сфере информационных технологий, что приводит к противоречиям правоприменительной практики. Исходя из этого, существует объективная необходимость в принятии Постановления Пленума Верховного Суда Российской Федерации по делам о преступлениях в сфере информационных технологий.

Таким образом, поставленная в начале исследования цель – достигнута, все задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нормативно-правовые акты и материалы правоприменительной практики

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.09.2022) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954; Собрание законодательства РФ, 26.09.2022, № 39, ст. 6535.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 07.10.2022) // Собрание законодательства Российской Федерации. 2001. № 52 (I часть). Ст.4921.

4. Федеральный закон от 02.12.1990 № 395-1 (ред. от 14.07.2022) «О банках и банковской деятельности» // Собрание законодательства РФ, 05.02.1996, № 6, ст. 492; Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5259.

5. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 28.06.2022) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ, 14.08.1995, № 33, ст. 3349; Собрание законодательства РФ, 04.07.2022, № 27, ст. 4603.

6. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 30.12.2021) «О связи» (с изм. и доп., вступ. в силу с 01.05.2022) // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895; Собрание законодательства РФ, 03.01.2022, № 1 (Часть I), ст. 34.

7. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448; Собрание

законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5292.

8. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 21.12.2021) «О полиции» // Собрание законодательства РФ, 14.02.2011, № 7, ст. 900; Собрание законодательства РФ, 27.12.2021, № 52 (часть I), ст. 8983.

9. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // Собрание законодательства РФ", 11.04.2011, N 15, ст. 2036. Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5306.

10. Федеральный закон от 28.12.2013 № 395-ФЗ (ред. от 30.12.2020) «О Государственной автоматизированной информационной системе «ЭРА-ГЛОНАСС» // Собрание законодательства РФ, 30.12.2013, № 52 (часть I), ст. 6960; Собрание законодательства РФ, 04.01.2021, № 1 (часть I), ст. 27.

11. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ, 11.07.2016, № 28, ст. 4558.

12. Федеральный закон от 29.07.2017 № 245-ФЗ (ред. от 05.12.2017) «О внесении изменений в Федеральный закон «О связи» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4794.

13. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ, 15.05.2017, № 20, ст. 2901.

14. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700.

15. Постановление Правительства РФ от 25.08.2008 №641 (ред. от 12.11.2016) «Об оснащении транспортных, технических средств и систем

аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» // Собрание законодательства РФ, 01.09.2008, № 35, ст. 4037; Собрание законодательства РФ, 21.11.2016, № 47, ст. 6640.

16. Постановление Правительства РФ от 23.09.2017 № 1145 «О Межведомственной комиссии по внедрению и развитию систем аппаратно-программного комплекса технических средств «Безопасный город», системы обеспечения вызова экстренных оперативных служб по единому номеру "112" и Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС» // Собрание законодательства РФ, 02.10.2017, № 40, ст. 5850.

17. Постановление Правительства РФ от 02.03.2019 № 234 (ред. от 13.05.2022) «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с "Положением о системе управления реализацией национальной программы «Цифровая экономика Российской Федерации») // Собрание законодательства РФ, 18.03.2019, № 11, ст. 1119; Собрание законодательства РФ, 23.05.2022, № 21, ст. 3443.

18. Распоряжение Правительства РФ от 03.12.2014 № 2446-р (ред. от 05.04.2019) «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // Собрание законодательства РФ, 15.12.2014, № 50, ст. 7220.

19. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ, 31.08.2020, № 35, ст. 5593.

20. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] Режим доступа: http://www.consultant.ru/.

21. Приказ МВД России от 17.01.2006 № 19 (ред. от 28.12.2021) «О

деятельности органов внутренних дел по предупреждению преступлений» (вместе с «Инструкцией о деятельности органов внутренних дел по предупреждению преступлений») // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

22. Приказ МВД России от 15.06.2021 № 444 (ред. от 28.12.2021) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

23. Распоряжение МВД России от 11.01.2022 № 1/37 (ред. от 30.06.2022) «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022-2024 годы» // Министерство внутренних дел Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

24. Паспорт федерального проекта «Цифровое государственное управление» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: Официальный сайт [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/.

25. Приговор Шадринского районного суда Курганской области от 20 июля 2021 г. № 1-295/2021 по делу № 1-295/2021 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/jW6qdZvy7nY4/.

26. Приговор Малодербетовского районного суда республики Калмыкии от 28 марта 2022 г. по делу №1-4 (2022) (1-77/2021) //

Официальный сайт Малодербетовского районного суда Республики Калмыкия [Электронный ресурс]. Режим доступа – http://maloderbetovsky.kalm.sudrf.ru/.

27. Решение Октябрьского районного суда г. Тамбова № 12-524/2017 от 28 сентября 2017 г. по делу № 12-524/2017 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/nyHN1d6cw7ri/.

28. Решение Ярославского областного суда от 6 июля 2021 г. № 3А-451/2021 3А-451/2021~М-268/2021 М-268/2021 по делу № 3А-451/2021 // Судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/regular/doc/jW6qdZvy7nY4/.

2. Специальная литература

29. Белкин А.Р. Теория доказывания в уголовном судопроизводстве. В 2 ч. Часть 2: учеб. пособие для вузов / А. Р. Белкин. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2019. – 294 с.

30. Большая советская энциклопедия. Том 10. Ива - Италики. 3-е изд. / Глав. ред. А. М. Прохоров. – М.: Сов. энциклопедия, 1972. – 592 с.

31. Голубовский В.Ю. Теория и практика информационного обеспечения оперативно-розыскной деятельности подразделений криминальной милиции: автореферат дис. ... доктора юридических наук: 12.00.09 / С.-Петерб. ун-т МВД РФ. – Санкт-Петербург, 2001. – 50 с.

32. Даль В.И. Толковый словарь живого великорусского языка : избр. ст. / В.И. Даль; совмещ. ред. изд. В.И. Даля и И.А. Бодуэна де Куртенэ. – М.: Олма-Пресс: Крас. пролетарий, 2004. – 700 с.

33. Ищенко Е.П., Топорков А.А. Криминалистика: учебник / под ред. Е.П. Ищенко. 2-е изд., испр., доп. и перераб. М.: КОНТРАКТ, ИНФРА-М, 2010. – 784 с.

34. Лазарева В.А. Доказывание в уголовном процессе : учебник для бакалавриата и магистратуры / В. А. Лазарева. – 7-е изд., перераб. и доп. –

М. : Издательство Юрайт, 2019 – 263 с.

35. Страхов А.А., Слесарева Е.А., Задохина Н.В. Информационные технологии в ОВД. Основные термины и определения: словарь / М.: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. – 104 с.

36. Хлебников А.А. Информационные технологии (для бакалавров). М.: КноРус, 2016. С. 116.

37. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. – Москва: Издательство Юрайт, 2022. – 417 с.

3. Публикации в периодических изданиях

38. Антонян Ю.М. Общая концепция предупреждения преступности // Человек: преступление и наказание. 2013. №3. С. 16-22.

39. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. №2 (104). С. 43-49.

40. Бецков А.В. О научно-технической политике мвд россии до 2030 года // НиКа. 2020. №. С. 26-29.

41. Валединская Е. Н., Астафьева О. А., Бочарова Э. А. Специфика эффективного маркетинга в социальных сетях // Дискуссия. 2017. № 3. С. 22–26.

42. Ваценко А.А. Обзор техник компьютерной криминалистики // Бюллетень науки и практики. 2020. №6. С. 167-180.

43. Великородный П.Г. Сокрытие следов преступления и противодействие его расследованию как способ уклонения от уголовной ответственности // Вестник СГЮА. 2018. №2 (121). С. 180-187.

44. Вехов В.Б. Основные направления использования компьютерных технологий в деятельности следователя // Информационная безопасность регионов. 2007. №1. С. 47-54.

45. Демидченко Ю.В. Снятие информации с технических каналов связи как один их способов получения сведений, используемых в процессе доказывания по уголовному делу // Вестник юридического факультета Южного федерального университета. 2021. №4. С. 67-74.

46. Диденко К.В. Некоторые проблемы выявления и предупреждения киберпреступлений // Вестник БелЮИ МВД России. 2020. №3. С. 20-24.

47. Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения // Известия ТулГУ. Экономические и юридические науки. 2017. №2-2. С. 24-30.

48. Ишин А.М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. 2016. №4. С. 21-28.

49. Комардина А.А., Меняйло Д.В., Меняйло Л.Н. Применение информационных технологий и возможностей цифровизации в деятельности сотрудника ОВД // В сборнике: Экономическая безопасность: правовые, экономические, экологические аспекты. Сборник научных трудов 6-й Международной научно-практической конференции. Курск, 2021. С. 184-187.

50. Костенко Н.С., Семененко Г.М., Пшеничкин А.А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе // Вестник ВИ МВД России. 2020. №4. С. 192-195.

51. Лаврик О.Л., Калюжная Т.А. Содержание понятий «информационное обеспечение», «информационное сопровождение», «поддержка научных исследований» как этапы информационного обслуживания ученых // Вестн. Том. гос. ун-та. Культурология и искусствоведение. 2020. №40. С. 305-319.

52. Лаврушкина А.А. Типичные следственные действия в рамках методики расследования мошенничества с использованием сети Интернет и средств мобильной связи // Бюллетень науки и практики. 2018. №4.

[Электронный ресурс] Режим доступа: URL:https://cyberleninka.ru/article/n/tipichnye-sledstven.

53. Лещенко А.М. Мультифункциональность сетевых коммуникаций в современном обществе // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2011. №2. С. 129-134.

54. Маилян А.В. Особенности возбуждения уголовного дела о хищении,совершенном с использованием электронных средств платежа // Вестник Сибирского юридического института МВД России. 2021. №2 (43). С. 30-37.

55. Максимова В.П. Формы, методы и направления использования специальных знаний в целях выявления и преодоления противодействия расследованию преступлений // Юридическая наука и правоохранительная практика. 2017. №3 (41). С. 197-200.

56. Малышева И.В. Использование современных информационных технологий в деятельности оперативных подразделений полиции при раскрытии имущественных преступлений // В сборнике: Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы международной научно-практической конференции. Составитель Э. Х. Мамедов. 2019. С. 574-577.

57. Михайлова М.С. Отдельные вопросы проведения портретной экспертизы в рамках криминалистического исследования // Международный журнал гуманитарных и естественных наук. 2019. №11-3. С. 34-42.

58. Намруева Э. В. Использование социальных сетей в деятельности подразделений информации и общественных связей органов внутренних дел: отечественный и зарубежный опыт // Вестник Московского университета МВД России. 2018. № 3. С. 34–38.

59. Овсянников И.В. Доказательственное значение актов ревизий и документальных проверок // Вестник ВИ МВД России. 2012. №4. С. 36-41.

60. Плахота К.С. К вопросу об использовании высоких технологий в

расследовании преступлений // Расследование преступлений: проблемы и пути их решения. 2021. №3(33). С. 146-152.

61. Погодина И.В., Лазарева К.А. Организация контроля пассажиров в аэропортах Российской Федерации // Туризм: право и экономика. 2019. № 1. С. 26-28.

62. Салиев А.А. К понятию о роли специальных знаний используемых в ходе расследования преступлений // European journal of law and political sciences. 2016. №4. С. 76-80.

63. Сафонов А.А. Современная автоматизированная дактилоскопическая идентификационная система органов внутренних дел российской федерации // Вестник экономической безопасности. 2021. №3. С. 179-183.

64. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6. С. 178-185.

65. Созаева А.С. Использование новых информационных технологий в раскрытии и расследовании преступлений // В сборнике: Право в эпоху информационных технологий: проблемы и пути решения. Сборник материалов международной научно-практической конференции среди студентов, магистрантов и аспирантов. Пермь, 2021. С. 200-204.

66. Степанова М.А., Царёв Е.В. Проблемы определения места совершения хищения денежных средств с использованием информационнотелекоммуникационных технологий // Вестник БелЮИ МВД России. 2021. №1. С. 12-16.

67. Степанян А.И. Предиктивная аналитика в прогностической деятельности полиции современных государств // Вестник Санкт-Петербургского университета МВД России. 2019. №4 (84). С. 43-50.

68. Сухов А.В., Конюшев В.В. Цифровая полиция как эргатическая система, функционирующая в цифровой экосистеме // Правовая информатика. 2021. №2. С. 28-38.

69. Терехов А.М. Моделирования и прогнозирования преступности: теоретический аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. №2 С. 123-127.

70. Тишутина И.В. Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Известия ТулГУ. Экономические и юридические науки. 2019. №4. С. 46-55.

71. Токбаев А.А., Кудрявцев С.В., Несмелов П.В. Применение информационных технологий в деятельности ОВД // В сборнике: Актуальные вопросы тактико-специальной подготовки сотрудников правоохранительных органов. Сборник статей предназначен для научных работников, педагогических работников, курсантов и слушателей образовательных организаций системы МВД России Сборник статей по итогам научно-практической конференции под редакцией В.Н. Гонтаря. 2020. С. 106-111.

72. Фетисов А.В., Никитин Д.В. К вопросу использования современных специальных средств с применением информационных технологий в деятельности ОВД // В сборнике: Современные подходы к подготовке сотрудников ОВД к действиям при возникновении чрезвычайных обстоятельств. Сборник научных статей реферативных чтений, посвящённых дню Российской науки кафедры ДОВД в ОУ УНК СП Московского университета МВД России имени В.Я. Кикотя. Под общей редакцией В.Н. Гонтаря. 2019. С. 196-205.

73. Харисова З.И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник УЮИ. 2019. №3 (85). С. 92-98.

74. Шаров В.И. Оперативно-розыскные мероприятия в сети интернет // Общество и право. 2018. № 2 (64). С. 82-87.

75. Эмиров М.Б., Саидов А.Г., Рагимханова Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Дагестанского государственного университета. 2011. №2. С. 63-66.

4. Интернет-источники

76. Государственная автоматизированная система Российской Федерации «Правосудие» интернет-портал [Электронный ресурс]: Режим доступа – https://sudrf.ru/.

77. Официальный сайт Управления Министерства Внутренних Дел России по Орловской области [Электронный ресурс]: Режим доступа – http://57.мвд.рф.

78. Официальный интернет-портал правовой информации [Электронный ресурс]: Режим доступа – на Официальном интернет-портале правовой информации http://www.pravo.gov.ru.

79. Официальный интернет-сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – Режим доступа: https://мвд.рф/.

80. Официальный сайт Центрального Банка Российской Федерации [Электронный ресурс]. – Режим доступа: https://cbr.ru/.