На правах рукописи

Павлюков Виталий Владимирович

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Специальность: 5.1.4. Уголовно-правовые науки
(юридические науки)

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2025

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Кубанский государственный аграрный университет имени И. Т. Трубилина»

Научный руководитель: **Швец Сергей Владимирович**
доктор юридических наук, доцент

Официальные оппоненты: **Вехов Виталий Борисович**
доктор юридических наук, профессор,
ФГАОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», профессор кафедры «Безопасность в цифровом мире»

Поляков Виталий Викторович
кандидат юридических наук, доцент,
ФГБОУ ВО «Алтайский государственный университет», доцент кафедры уголовного процесса и криминалистики

Ведущая организация: **ФГАОУ ВО «Севастопольский государственный университет»**

Защита диссертации состоится 27 ноября 2025 г. в $10^{\underline{00}}$ часов на заседании диссертационного совета 35.2.019.01 на базе ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», по адресу: 350044, г. Краснодар, ул. Калинина, 13, главный учебный корпус, ауд. 215.

С диссертацией можно ознакомиться в библиотеке университета и на сайтах: ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина» – www.kubsau.ru и ВАК – https://vak.minobrnauki.gov.ru

Автореферат разослан «___» _____2025 г.

Ученый секретарь
диссертационного совета,
кандидат юридических наук С.И.Грицаев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность научного исследования. В настоящее время компьютерные технологии расширяют возможности получения, использования и передачи информации. Однако, помимо своих положительных качеств, они способствуют росту преступности как в киберпространстве, так и в реальном мире.

Правоохранительные органы, получая информацию преимущественно путем поверхностного мониторинга социальных сетей и изучения сообщений в мессенджерах, упускают из виду возможности современных аналитических систем и специальных программно-аппаратных комплексов. Происходит это потому, что на законодательном уровне недостаточно разработаны механизмы, позволяющие правоохранительным органам получать и оперативно использовать компьютерную информацию в целях противодействия преступности. Назрела необходимость как законодательного закрепления более действенных способов использования правоохранительными органами потенциала современных компьютерных технологий в расследовании преступлений, так и усовершенствования существующих методик, а также тактических приемов получения компьютерной информации.

Проведенный диссертантом анализ ситуации, связанный с получением компьютерной информации, используемой в расследовании преступлений, построенный на базе статистических данных и научно-исследовательских работ, а также в связи с быстрой адаптацией злоумышленников к современным технологиям с целью повышения собственной эффективности, позволяет сделать выводы о необходимости постоянного совершенствования тактики получения компьютерной информации. Данные, предоставленные Министерством внутренних дел (далее – МВД) Российской Федерации (далее – РФ), только подтверждают факт того, что, несмотря на существующие методики и тактические приемы, количество преступлений, совершаемых в сфере компьютерной информации, постоянно растет. За 12 месяцев 2024 года зарегистрировано 765,4 тысячи киберпреступлений, что на 13,1% больше, чем за аналогичный период 2023 года. Примечательно то, что в целом на деяния, совершенные с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, приходится 40% зарегистрированных преступлений[1]. При всем этом способы и методы совершения преступлений при помощи компьютерной информации претерпевают значительные изменения, а существующие тактики расследования являются точечными и устаревшими.

Поэтому актуальным видится разработка новых организационных и тактических приемов установления источников компьютерной информации,

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года [Электронный ресурс] Сайт МВД РФ // Режим доступа: URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 18.02.2025).

используемых программных средств, при помощи которых осуществлялось ее создание и распространение, а также усовершенствование способов идентификации причастных к такой информации пользователей в комплексе с изучением возможностей современного программного обеспечения.

Необходимо отметить, что важным условием в деле повышения эффективности противодействия преступлениям, совершаемым при помощи компьютерной информации, является использование всех доступных возможностей современных программных комплексов и сервисов, внедрение искусственного интеллекта в процесс расследования, в том числе с задействованием существующих у МВД России информационно-справочных учетов. Научное осмысление данного аспекта проблемы, на наш взгляд, способно привести к разработке более действенной организации получения и более результативного использования сотрудниками правоохранительных органов компьютерной информации в процессе расследования преступлений.

Вышеизложенное указывает на практическую актуальность и недостаточную теоретическую разработку обозначенной проблемы, что, безусловно, требует ее научного разрешения.

Степень научной разработанности темы исследования. Проблематика использования компьютерной информации, ее обнаружения и фиксации при расследовании преступлений была направлена на выявление противоправных деяний, совершаемых непосредственно в компьютерной сети. В последнее время только начинают появляться научные работы, где сфера информационных технологий стала пристально рассматриваться как источник получения компьютерной информации о преступлениях не только в виртуальном, но и в реальном мире. К последним можно отнести диссертации А.Н. Колычевой «Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет» (2018 год), Н.С. Зиновьевой «Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений» (2020 год) и Е.А. Хариной «Особенности методики расследования мошенничества в сфере компьютерной информации» (2024 год). Однако существующие диссертационные исследования являются точечными, где получение компьютерной информации описано лишь на отдельных этапах расследования или по отдельным преступлениям.

Проблематика получения и использования информации об отдельных преступлениях, совершаемых при помощи компьютерной информации, освещалась в работах А.Б. Смушкина, В.Б. Вехова, Р.Н. Вязовца, А.М. Ишина, А.В. Касаткина, Н.Н. Лыткина, В.А. Мещерякова, Д.В. Огородова, А.Л. Осипенко, М.А. Простосердова, О.А. Решняка, В.А. Родивилиной, П.Г. Смагина, В.Г. Степанова-Егиянца, А.В. Суслопарова и др.

Внимания также заслуживают научные публикации, посвященные организации расследования преступлений. В последних авторы затрагивают вопросы использования компьютерной информации в расследовании преступлений. К таким работам можно отнести исследования В.В. Крылова, Ю.В. Гаврилина, В.Д. Зеленского, Г.М. Меретукова, П.С. Пастухова, Е.Р. Россинской, А.Д. Ульянова, С.В. Швеца, Н.Л. Щеголевой, Р.Х. Якупова и

др.

В то же время сложность проблемы, недостаточная разработанность ее отдельных аспектов, а также проведенные в последние годы научные исследования обусловливают необходимость дальнейшего детального рассмотрения указанных вопросов, связанных с использованием компьютерной информации в расследовании преступлений.

Объектом диссертационного исследования является деятельность правоохранительных органов, направленная на получение и использование компьютерной информации в процессе расследования преступлений.

Предметом диссертационного исследования являются закономерности использования компьютерной информации в процессе расследования преступлений.

Целью диссертационного исследования является анализ теоретических, практических и организационно-тактических особенностей получения и использования компьютерной информации в расследовании преступлений. Такая деятельность заключается в разработке современных научно обоснованных аспектов и выработке практических рекомендаций по тактике получения, фиксации и использования компьютерной информации в расследовании преступлений.

Для достижения этой цели были поставлены и решались следующие задачи:

1. В спектре деятельности правоохранительных органов по расследованию преступлений сделать более современным содержание научных подходов к интерпретации понятий «информация», «компьютерная информация», «данные» и «компьютерная информация, используемая в расследовании преступлений».
2. Структурировать и выделить наиболее актуальные источники компьютерной информации, имеющей значение для расследования преступлений.
3. На основании передового зарубежного опыта регулирования получения подразделениями правоохранительных органов компьютерной информации в целях расследования преступлений сформулировать рекомендации по его внедрению в российскую нормотворческую практику.
4. Раскрыть особенности организации получения компьютерной информации в процессе расследования преступлений.
5. Усовершенствовать взаимодействие следственных и оперативно-розыскных подразделений при получении и использовании компьютерной информации, имеющей значение для расследования преступлений.
6. Охарактеризовать тактические особенности использования компьютерной информации при подготовке и проведении отдельных следственных действий и оперативно-розыскных мероприятий.
7. Сформулировать рекомендации по применению современных программных продуктов, искусственного интеллекта и информационно-справочных систем правоохранительных органов РФ в целях получения компьютерной информации, имеющей значение для расследования преступлений, используя вневедомственные источники (операторов связи и

организаторов распространения информации в сети Интернет).

Все вышеуказанное, в свою очередь, требует освещения разнообразных вопросов, связанных с исследованием криминогенной сферы компьютерной информации, разрешением научных и практических проблем, где необходимо акцентировать свое внимание именно на возможности использования сотрудниками органов внутренних дел (далее – ОВД) компьютерной информации в расследовании преступлений, ее поиске, получении из различных информационных компьютерных систем, в том числе и таких, где доступ к компьютерным данным ограничен.

Методология и методика исследования. Научная аргументация теоретических выводов и положений, представленных в диссертации, базируется на современных разработках различных отраслей науки.

В процессе исследования использовались следующие методы:

- диалектический – обеспечил исследование отдельных ключевых категорий и понятий, позволил выявить как внешние, так и внутренние связи специальных, технологических, организационных и правовых явлений и процессов, развитие и взаимосвязь объектов реальной действительности;

- статистический – позволил осуществить сбор и анализ статистических данных, касающихся раскрытия и расследования преступлений с использованием компьютерной информации, изучить судебные решения, где указывалось о получении и использовании компьютерной информации в процессе расследования преступлений;

- сравнительно-правовой – при изучении нормативной и правовой регламентации деятельности отечественных и зарубежных подразделений правоохранительных органов, полицейских структур зарубежных стран, связанной с получением и использованием компьютерной информации в расследовании преступлений;

- моделирования – при разработке и внедрении в практику алгоритмов и методических рекомендаций для осуществления противодействия преступности и тактических особенностей использования компьютерной информации в расследовании преступлений.

Вместе с тем использовались и специальные методы криминалистики, такие как метод планирования расследования при изучении фактических данных о преступлениях, совершаемых в сфере компьютерной информации с дальнейшим выдвижением версий для установления полного представления о происходящих действиях злоумышленника с компьютерной информацией; технико-криминалистические методы с целью сбора и исследования доказательственной компьютерной информации; метод идентификации с целью установления причинно-следственной связи между пользователем и компьютерной информацией.

Нормативной и правовой базой исследования послужило отечественное и зарубежное законодательство, а именно: Конституция РФ, конвенции и директивы, регулирующие вопросы расследования преступлений при помощи компьютерной информации (преступлений как против компьютерных систем и сетей, так и с их использованием), нормы действующего уголовного и уголовно-

процессуального законодательства, а также иные нормативные федеральные законы (далее – ФЗ) РФ (законы «О полиции», «О связи», «Об оперативно-розыскной деятельности», «Об информации, информационных технологиях и о защите информации») и иные нормативные и правовые акты, касающиеся вопросов регулирования и доступа к компьютерной информации, представляющей интерес при расследовании преступлений.

Научно-теоретической базой диссертационного исследования послужили научные труды в области криминалистики, оперативно-розыскной деятельности, уголовного права, уголовно-процессуального права.

Эмпирическую базу исследования составляют результаты анкетирования 100 оперативных сотрудников и следователей ОВД Луганской Народной Республики (далее – ЛНР), Донецкой Народной Республики (далее-ДНР), г. Севастополя, контент-анализ 60 судебных дел открытой судебной практики РФ о преступлениях, где компьютерная информация использовалась в расследовании преступлений; результаты изучения статистических данных о состоянии преступности с использованием компьютерной информации; данные, полученные в ходе анкетирования, эмпирические исследования ученых; личный практический опыт в должности как оперативного сотрудника, так и сотрудника Управления информационно-аналитического обеспечения МВД, где одним из основных направлений было использование информационно-справочных систем МВД с целью противодействия преступлениям, совершаемым при помощи компьютерной информации.

Научная новизна диссертационного исследования заключается в проведении на монографическом уровне комплексного исследования наиболее актуальных вопросов, связанных с разработкой и внедрением тактики получения и использования компьютерной информации в процессе расследования.

В работе получили дальнейшее развитие теоретические положения, которые относятся к исследуемой проблеме, а именно: внедрение унифицированной программно-аппаратной системы для поиска и фиксации значимой для расследования компьютерной информации в сети Интернет. Предложено и обосновано использование такого оперативно-розыскного мероприятия (далее – ОРМ), как «Компьютерная разведка», а также сформулированы рекомендации по применению ОРМ «Получение компьютерной информации». Полученные выводы могут использоваться в дальнейших научных разработках методик получения компьютерной информации в деятельности ОВД.

Научная новизна диссертационного исследования нашла отражение в следующих его положениях, выносимых на защиту:

1. Уточнены понятия «компьютерная информация» и «данные», а также предложено определение «компьютерная информация, используемая в расследовании преступлений». Под последней следует понимать совокупность данных, находящихся на компьютерных носителях или передаваемых при помощи компьютерных сетей и систем, имеющих значение для выявления и раскрытия преступлений, которые возможно получить и зафиксировать в процессе проведения определенных оперативно-розыскных мероприятий,

следственных и иных законных действий сотрудников ОВД. Акцентируется внимание на том, что не следует путать понятия «Компьютерная информация» и «данные», где данные – это та информация, которая хранится, преобразуется и передается при помощи компьютерных систем в цифровом виде и которую человек не способен понять. Для того, чтобы правоохранительные органы имели реальную возможность использовать компьютерную информацию в целях эффективного решения поставленных задач, компьютерная информация разграничена по следующим признакам: трансграничность; неисчерпаемость; измеримость; трансформируемость; доступность; защищенность; обезличенность; автоматизация обработки.

2. Предложена классификация источников компьютерной информации, которая должна учитываться в процессе расследования преступлений, а именно: по способу передачи, по способу представления, по способу хранения, по способу шифрования, по способу доступа.

Эффективность практической деятельности по раскрытию и расследованию преступлений можно повысить за счет: а) использования компьютерной информации из открытых источников и источников с ограниченным доступом; б) модернизации механизма получения информации у интернет- и хостинг-провайдеров, владельцев интернет-ресурсов с учетом специфики задач, которые возлагаются на подразделения правоохранительных органов; в) разработки специальных информационных систем в ОВД, где будет накапливаться и анализироваться компьютерная информация, имеющая значение для расследования преступлений.

3. На основании анализа зарубежного опыта нормативного и правового регулирования, а также судебной практики Российской Федерации сформулированы предложения и рекомендации для правоохранительных органов РФ получать значимую для расследования информацию путем удаленного доступа к базам данных государственных органов и государственных внебюджетных фондов.

4. Раскрыты особенности организации способов получения компьютерной информации в целях раскрытия преступлений и охарактеризовано содержание отдельных типичных версий, которые могут применяться следователями при расследовании преступлений, в частности, в зависимости от следующих ситуаций:

- наличия информации в ведомственных и базах данных других организаций и учреждений;
- физического места нахождения информационного источника;
- состояния технического средства, содержащего компьютерную информацию;
- специализации в области информационных технологий владельца информационного источника или пользователя программного обеспечения.

5. Определены основные формы взаимодействия следственных и оперативно-розыскных подразделений с учетом поиска и использования компьютерной информации, имеющей значение для расследования преступлений. Доказана целесообразность расследования преступлений в сфере

компьютерной информации без привлечения специалиста, но с учетом использования соответствующих методов получения компьютерной информации.

6. В процессе проведения оперативно-розыскной деятельности (далее – ОРД) помимо использования существующих ОРМ, с целью получения компьютерной информации предложено такое мероприятие, как «Компьютерная разведка», которая даст возможность преодолевать программную защиту на удаленных интернет-ресурсах путем получения информации от злоумышленников при помощи сети Интернет. В данном случае, тактическим приемом с целью получения компьютерной информации, имеющей значение для расследования, будет создание и использование собственного сайта (фишингового сайта).

Определены тактические особенности использования компьютерной информации при подготовке и осуществлении таких отдельных следственных действий, как осмотр и допрос.

7. Для решения криминалистических задач предложено внедрение искусственного интеллекта в процесс расследования преступлений в сфере компьютерной информации. Обоснована необходимость интеграции компьютерной информации о пользователе и его действиях из вневедомственных компьютерных систем в банки данных ОВД.

Теоретическая и практическая значимость полученных результатов. Результаты диссертационного исследования могут быть внедрены в практику противодействия преступлениям, совершаемым при помощи компьютерной информации. В работе проанализировано и раскрыто понятие ОРМ «Получение компьютерной информации», предложено новое ОРМ «Компьютерная разведка», где была учтена возможность доступа к компьютерной информации.

Полученные результаты содержат научно обоснованные и практически подтвержденные предложения автора, которые могут использоваться: при подготовке учебной и научной литературы; при разрешении проблем, связанных с получением информации; в целях повышения эффективности расследования преступлений, совершаемых с использованием компьютерной информации.

Практическое значение результатов исследования. Указанные в работе положения, выводы и предложения могут быть применены для повышения эффективности:

- практической деятельности правоохранительных органов – как рекомендации по совершенствованию способов и тактики получения компьютерной информации, ее фиксации и использования в расследовании преступлений;

- научно-исследовательской работы – как основы для дальнейших научных усовершенствований организационно-правовых основ получения компьютерной информации и ее использования в ходе расследования преступлений;

- учебного процесса – при подготовке учебно-методической литературы и проведении занятий по криминалистике, ОРД и основам кибербезопасности.

Апробация и внедрение результатов диссертационного исследования. Основные положения работы, выводы, предложения и рекомендации

обсуждались на заседании кафедры криминалистики ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина».
Результаты диссертационного исследования были представлены на XI Всероссийской научной конференции молодых ученых «Наука. Технологии. Инновации» (2017, г. Луганск (ЛАВД им. Э.А.Дидоренко), Международной научно-практической конференции «Юридический факультет КубГУ: 60 лет служения науке и практике» (2018, г. Краснодар КубГУ), Международной научно-практической конференции (к 25-летию Луганской академии внутренних дел имени Э.А. Дидоренко) «Молодежь в науке: настоящее и будущее» (2018, г. Луганск (ЛАВД им. Э.А.Дидоренко), Юбилейной Всероссийской научно-практической конференции с международным участием «Современные проблемы отечественной криминалистики и перспективы ее развития», посвященной 20-летию кафедры криминалистики ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина» (2018, г. Краснодар (КубГАУ), Международной научно-практической конференции «Охрана, безопасность, связь» (2024, г. Воронеж (ВИ МВД России).

По теме диссертации опубликованы 12 статей, 9 из которых в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ.

Рекомендации и предложения, содержащиеся в материалах диссертации, внедрены в практическую деятельность Артемовского районного отделения МВД ЛНР, нашли применение в учебном процессе при подготовке учебно-методического пособия по дисциплине «Криминалистика» Луганского филиала Воронежского института МВД России, а также используются в учебном процессе кафедры криминалистики ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина».

Структура работы. Диссертационная работа состоит из введения, трех глав, включающих девять параграфов, заключения, списка литературы и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, определяются ее связь с научными планами и программами, цель и задачи, объект и предмет, методы исследования, научная новизна и практическое значение полученных результатов, апробация результатов диссертации и публикации.

Первая глава диссертации **«Характеристика компьютерной информации, используемой в расследовании преступлений»** содержит три параграфа.

В первом параграфе «Понятие и признаки компьютерной информации, используемой в расследовании преступлений» отмечено, что в существующих научных исследованиях и действующем законодательстве Российской Федерации недостаточно полно отражен перечень и раскрыто содержание признаков современной компьютерной информации, что требует более

детального изучения и разработки на основе соответствующего анализа понятия последней, пригодного для практического использования в ОВД.

Ознакомление с научными исследованиями по проблематике диссертации позволило выявить два главных вектора, по которым происходит оперирование понятием «компьютерная информация» в приложении к противоправной деятельности, а именно:

первый – преступления, совершаемые при помощи компьютерной информации, компьютерных сетей и систем, именуют «компьютерные преступления»;

второй – преступления, совершаемые при помощи и против компьютерной информации, компьютерных систем и сетей только в информационной сфере, называют «киберпреступления».

Полагаем, что основными признакам компьютерной информации, используемой в расследовании преступлений, являются трансграничность, неисчерпаемость, измеримость, трансформируемость, защищенность, обезличенность, автоматизация обработки, ограниченность передачи радиусом действия компьютерных сетей и систем, возможность преобразования из одной объектной формы в другую, сохраняемость в первоисточнике после ее изъятия, одновременная доступность нескольким пользователям.

Сделан вывод о том, что правоохранительным органам Российской Федерации для использования компьютерной информации в целях эффективного расследования преступлений необходимо на законодательном уровне четко нормативно зафиксировать (прежде всего, в ФЗ «Об информации, информационных технологиях и о защите информации») следующие понятия: «компьютерная информация», «данные» и «компьютерная информация, используемая в расследовании преступлений». В соответствии с этим обоснованы и даны авторские определения указанных понятий.

Во втором параграфе «Источники компьютерной информации, используемой в расследовании преступлений» на основе анализа научных исследований и судебной практики указывается, что наиболее доступным и быстро развивающимся источником компьютерной информации, используемой в расследовании преступлений, в настоящее время являются компьютерные сети и системы, банки данных учреждений, организаций и предприятий, а также иные организаторы распространения информации в сети Интернет (хостинг- и интернет-провайдеры).

Отмечается, что, используя компьютерные сети и системы, преступник оставляет компьютерные следы на компьютерных устройствах, периферийных и сетевых устройствах, ресурсах сети Интернет. Файлы с данными, а также программное обеспечение, которое подвергается преступным посягательствам, становятся носителями следовой информации.

Телекоммуникационные каналы служат для передачи, как правило, двух видов информации: адресной, определяющей адрес получателя информации, и сообщения. При расследовании преступлений больший интерес, чаще всего, вызывает само сообщение, поступающее с интересующего адреса и несущее в себе сведения о преступлении. Но зачастую не меньшее значение имеет и

адресная информация, способная сориентировать правоохранителей на связях преступника, времени и месте совершения преступления.

Следы от противоправной деятельности, остающиеся в каналах связи, – это сведения о переданных сообщениях, накапливаемые в передающем оборудовании и фиксируемые в специальных файлах (Log-файлах).

Обосновано, что к провайдерам и владельцам хостинга необходимо относиться как к источникам информации, которая может иметь значение в расследовании преступлений. Предложено, чтобы такая информация сохранялась в текстовом Log-файле и передавалась на выделенный удаленный сервер хранения Log-файлов МВД для оперативно-аналитических целей, не нарушающих частную жизнь граждан.

В диссертационном исследовании предложена следующая классификация источников компьютерной информации, имеющая значение для расследования преступлений:

По способу передачи: Ethernet-кабели и USB-кабели; оптоволоконные кабели; радиоволны (Wi-Fi, Bluetooth, WIMAX и радиосвязь); сотовая связь.

По способу представления: числовой; текстовый; графический; звуковой.

По способу хранения:

- физические носители: накопитель на жёстком магнитном диске (HDD), твердотельные накопители (SSD);

- съемные носители: флеш-накопители, оптические диски (CD/DVD) и другие физические носители информации;

-удаленные источники: файловые серверы, сетевые хранилища (NAS), облачные хранилища, интернет - провайдеры, хостинг - провайдеры, Веб-серверы, серверы баз данных, системы геолокации (GPS), IP-камеры видеонаблюдения;

- резервные копии: RAID-массивы, локальные резервные копии данных, хранящиеся на отдельных устройствах или в виде образов дисков.

По способу шифрования:

- незашифрованные источники: информация, доступная без ограничений, например, публичные веб-сайты, открытые базы данных и т.д.;

- симметричное шифрование: источники, где данные шифруются одним и тем же ключом для шифрования и дешифрования. Примеры: файлы, зашифрованные с использованием алгоритмов AES, DES, Blowfish и т.д.;

- асимметричное шифрование: источники, использующие пару ключей: открытый и закрытый. Открытый ключ используется для шифрования, а закрытый – для дешифрования;

- гибридное шифрование: использование комбинаций симметричного и асимметричного шифрования. Пример: протоколы HTTPS;

- специализированные протоколы: протоколы, использующие шифрование для защиты данных: (SSL/TLS, VPN-протоколы);

-технологии шифрования данных на уровне файловой системы: такие технологии, как BitLocker (Windows) или FileVault (macOS).

По способу доступа:

- открытые источники, под которыми следует понимать такие, информация

в которых находится в свободном доступе для неограниченного круга лиц, то есть доступная для всех желающих получить ее. К таким можно отнести общедоступные ресурсы сети Интернет (социальные сети, открытые форумы и группы, новостные сайты, доски объявлений и т. д.);

- источники ограниченного доступа, а именно те, к которым владелец ресурса или пользователь ограничил доступ. К ним относятся ресурсы сети Интернет с ограниченным доступом и компьютерные устройства (стационарные компьютеры, ноутбуки, мобильные телефоны, планшеты, аудио- и видеорегистраторы, серверы, маршрутизирующее оборудование и т. д.), на которых оператор связи, интернет-провайдер, владелец интернет-ресурса, отдельный пользователь хранит информацию и защищает ее паролем или методами шифрования. Подчеркивается, что практически любую компьютерную информацию из открытой можно сделать с ограниченным доступом.

В третьем параграфе «Правовая регламентация доступа правоохранительных органов к компьютерной информации, используемой в расследовании преступлений: российский и зарубежный опыт» на основе анализа действующего законодательства РФ, а также зарубежного опыта таких государств, как Соединенные Штаты Америки (далее – США), Федеративная Республика Германия, Чешская Республика, Румыния, Королевство Швеция, Словацкая Республика, Соединенное Королевство Великобритания и Северная Ирландия, Королевство Дания, Республика Беларусь, Австралия, Французская Республика, Итальянская Республика, Китайская Народная Республика, Королевство Испания, Украина сделан вывод о том, что многие страны мира используют методы получения и доступа к компьютерной информации без судебного разрешения, а иногда и получают доступ к данным путем взлома, что закреплено на законодательном уровне. В свою очередь, российский правовой опыт содержит такие нормативные механизмы, которые усложняют процедуру получения значимых для расследования данных из компьютерной сети, из-за чего теряется их оперативность.

Указывается, что России стоит использовать в деле противодействия преступлениям в сфере информационных технологий весь позитивный опыт, который накоплен зарубежными странами. В частности, в Российской Федерации стоит создать более благоприятные условия для противодействия киберпреступности, а именно – оптимизировать механизм получения компьютерной информации, как это, например, реализовано в Австралии, где данные могут быть получены оперативным путем по средствам связи, а также при помощи различных программ и устройств. Стоит также изменить подход к хранению компьютерной информации в целесообразных временных рамках и только в отношении лиц, представляющих оперативный интерес (NSL-запросы в США) с обязательным соблюдением прав граждан.

С учетом отмеченного, можно заявить о том, что в ФЗ РФ «Об оперативно-розыскной деятельности» требуется внести дополнения о закреплении в нем возможности для правоохранительных органов получать удаленный доступ к компьютерной информации оперативного значения при наличии достаточных оснований и соответствующего судебного контроля. В статье 6 ФЗ РФ «Об

оперативно-розыскной деятельности» следует указать на то, что сотрудниками оперативных подразделений «В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде, позволяющие, в частности, получать необходимые для выполнения возложенных на оперативные подразделения обязанностей данные у операторов и организаторов распространения информации в сети Интернет путем запроса с использованием компьютерных систем и сетей, получать удаленный доступ к базам данных государственных органов и государственных внебюджетных фондов, за исключением случаев, когда федеральными законами установлен запрет на использование и передачу таких систем и (или) баз данных органам, осуществляющим оперативно-розыскную деятельность».

Вторая глава диссертации **«Организационные особенности получения компьютерной информации в целях расследования преступлений»** состоит из трех параграфов.

В первом параграфе «Особенности организации расследования преступлений с использованием компьютерной информации» указывается, что основу организации расследования преступлений с использованием компьютерной информации составляет планирование, которое осуществляется исходя из следующих версий:

1. В зависимости от наличия информации в ведомственных и вневедомственных базах данных:

а) компьютерная информация о расследуемом преступлении может находиться в ведомственных базах данных и криминалистических учетах МВД;

б) компьютерная информация о лице, причастном к совершенному преступлению, находится в различных банках данных учреждений, организаций или интернет-ресурсах, таких, как форумы по интересам, социальные сети, мессенджеры, у организаторов, предоставляющих услуги связи, а также интернет- и хостинг-провайдеров.

2. В зависимости от физического места нахождения информационного источника:

а) интересующая информация, имеющая значение для расследования преступления, содержится непосредственно на компьютерном устройстве, принадлежащем лицу, подозреваемому в совершении преступления;

б) интересующая компьютерная информация находится на компьютерном устройстве, не принадлежащем лицу, причастному к совершению преступления, однако при помощи которого был зафиксирован факт совершения преступления в момент или после его совершения.

3. В зависимости от состояния технического средства, содержащего компьютерную информацию:

а) компьютерная информация, представляющая интерес в расследовании, находится на поврежденном компьютерном устройстве;

б) компьютерная информация находится на заблокированном парольной защитой компьютерном устройстве или в зашифрованном виде;

в) источник компьютерной информации наличествовал, но был утерян или украден.

4. В зависимости от специализации в области информационных технологий владельца информационного источника или пользователя программного обеспечения:

а) компьютерная информация находится на электронном носителе, принадлежащем лицу, который является специалистом в области информационных технологий;

б) компьютерная информация содержит специфические сленговые выражения.

Во втором параграфе «Взаимодействие следственных и оперативно-розыскных подразделений при получении компьютерной информации в целях расследования преступлений» определены основные формы взаимодействия следственных и оперативно-розыскных подразделений с учетом поиска и использования компьютерной информации в расследовании преступлений. К таким относятся:

- совместный поиск и фиксация технических средств, программного обеспечения и иных источников, содержащих значимую для расследования информацию, а также лиц, которые имели отношение к созданию, распространению и хранению компьютерной информации, имеющей значение для расследования;

- совместное планирование, обеспечивающее организованность и согласованность всех действий в процессе расследования преступлений;

- взаимообмен информацией в целях качественной организации и проведения ОРМ, следственных действий;

- совместная постановка и разрешение тактических задач расследования, в том числе при использовании современного программного обеспечения, которое позволяло бы фиксировать и накапливать полученные в ходе расследования сведения на выделенном сервере МВД и должно быть доступным в режиме реального времени субъектам расследования.

Отмечается, что работу подразделений ОВД необходимо организовать так, чтобы любой сотрудник еще на подготовительном этапе мог получить компьютерную информацию, представляющую интерес, а затем с учетом ее строить план работы по раскрытию преступления, где такая информация использовалась. Для этого при помощи обращения с запросами к интернет-провайдеру, банкам, а также путем анализа имеющейся на компьютерном устройстве информации:

- выяснить, где и как приобреталось компьютерное оборудование, программное обеспечение путем анализа приложений для оплаты в сети Интернет;

- выявлять лиц, которые проявляют повышенный интерес к изучению специальной литературы, к примеру, относительно особенностей разработки и использования вредоносного программного обеспечения, используют ли они средства шифрования для выхода в сеть Интернет;

- путем анализа различных интернет-сервисов установить, пытался ли

пользователь приобрести или сбыть запрещенные к обороту товары и т. п.

Следователь с учетом информации, полученной из названных источников, в дальнейшем получает компьютерную информацию о расследуемом факте путем осуществления следственных действий.

В третьем параграфе «Получение компьютерной информации посредством использования специальных знаний» при рассмотрении особенностей использования специальных знаний для получения компьютерной информации обоснован вывод о необходимости задействования специалиста тогда, когда требуются его знания при работе со специальным программным обеспечением, в области программирования, а также для криминалистического исследования вещественных доказательств с целью обнаружения, фиксации и изъятия следов, оставленных в компьютере лицом, осуществляющим незаконные действия с компьютерной информацией. Указывается, что сотрудник ОВД может самостоятельно получить значимую для расследования компьютерную информацию, изучив и взяв на вооружение способы, используемые злоумышленниками.

Предлагаются авторские методики по получению компьютерной информации о злоумышленниках с применением фишингового сайта (при отсутствии признаков провокации), а также с использованием технологий искусственного интеллекта.

Третья глава диссертации **«Тактические особенности использования компьютерной информации в расследовании преступлений»** включает в себя три параграфа.

В первом параграфе «Организационно-тактические особенности расследования преступлений, совершаемых с использованием компьютерной информации» обращено внимание на проведение ОРМ «Наведение справок», «Получение компьютерной информации», «Снятие информации с технических каналов связи», «Прослушивание телефонных переговоров», где обосновывается необходимость совместного применения рассматриваемых мероприятий при получении компьютерной информации.

Критически оценивая взгляды ученых на понятие ОРМ «Получение компьютерной информации», автор считает, что указанное оперативно-розыскное мероприятие должно быть направлено на получение информации из компьютерных устройств, программного обеспечения, ресурсов сети Интернет путем их осмотра в целях фиксации противоправной деятельности определенных субъектов из открытых интернет-ресурсов без судебного решения, а в случае, если доступ к источнику информации закрыт, то при наличии соответствующего судебного решения или без него, но при добровольном согласии владельца компьютерной техники или пользователя ресурса сети Интернет.

Проведенное исследование также показало, что в большинстве случаев доступ к компьютерной информации является закрытым (она защищена паролем, зашифрована и т. д.). В связи с этим обосновывается целесообразность внесения дополнений в статью 6 ФЗ «Об оперативно-розыскной деятельности» в части расширения перечня оперативно-розыскных мероприятий за счет нового

ОРМ «Компьютерная разведка», направленного на санкционированное преодоление компьютерной защиты на удаленных интернет-ресурсах или же путем анонимного получения информации от злоумышленников при помощи сети Интернет в рамках предусмотренных законом процедур. Предлагается и описывается создание и использование собственного сайта (фишингового сайта) с целью получения компьютерной информации (метаданных), имеющей значение для расследования, при условии строгого соблюдения принципа отсутствия провокации и иных норм законодательства.

Во втором параграфе «Тактические особенности фиксации и использования компьютерной информации при осуществлении отдельных следственных действий» в ходе анализа судебной практики установлено, что фиксация компьютерной информации зачастую осуществляется путем снимка экрана смартфона или монитора компьютера (скриншота). Впоследствии составляется акт или протокол ОРМ, к которому прилагаются скриншоты, где также необходимо указать место, время, дату, фамилию и инициалы лица, сделавшего скриншот, примененные технические средства, условия и порядок их использования, объекты, к которым эти средства были применены, а также обеспечить возможность верификации подлинности полученных данных. Однако для придания таким результатам процессуальной формы и использования их в качестве доказательств необходимо будет процессуально фиксировать не только факт совершения противоправного действия, но также проводить всестороннее исследование информации, полученной у интернет- и хостинг-провайдеров, владельцев ресурсов в сети Интернет, обеспечивающее ее достоверность и неизменность. Это может способствовать успешному проведению таких следственных действий, как осмотр предмета (документа), выемка, а также допросы подозреваемого и свидетелей.

Полученная компьютерная информация может являться ориентиром для установления пользователя (Ф. И. О., IP-адрес, e-mail, номер мобильного телефона) и компьютерного устройства, при помощи которого совершалась противоправная деятельность (мобильный телефон, планшет, стационарный компьютер, сетевое оборудование и т. д.). Тактическим приемом будет демонстрация компьютерной информации при допросе, а именно – процессуально оформленная информация в виде распечатанного скриншота, которая может указывать не только на осведомленность об обстоятельствах, имеющих отношение к расследуемому событию, но также и на то, что эта информация уже надлежащим образом закреплена как доказательство.

В третьем параграфе «Особенности использования современных информационных технологий в практике расследования преступлений» для обеспечения возможности оперативного получения сотрудниками ОВД компьютерной информации обоснована необходимость совмещения данных, накопленных в учетах ОВД, с информацией, которая циркулирует в компьютерных сетях. Приводятся примеры из практики правоохранительных органов по задействованию искусственного интеллекта и нейросетей.

В целях законного использования и анализа при помощи информационных систем МВД информации, полученной из интернет-ресурсов, целесообразно

дополнить статью 17 ФЗ РФ «О полиции» пунктом следующего содержания: «Полиция имеет право вносить в банки данных и использовать в своей деятельности информацию о лицах, полученную из сети Интернет, при наличии законных оснований и с соблюдением требований о защите персональных данных».

Дополнительным подспорьем в деле противодействия киберпреступности может выступить обновленная редакция пункта 2 статьи 64 ФЗ РФ «О связи», которая зафиксирует, что операторы связи обязаны сохранять на территории Российской Федерации «на основании мотивированного запроса от правоохранительных органов в соответствии с федеральным законодательством 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».

В **заключении** диссертации подведены итоги исследования, сформулированы основные положения и выводы, имеющие определенное теоретическое и практическое значение для совершенствования деятельности по расследованию преступлений в сфере информационных технологий.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ:

Статьи в рецензируемых научных журналах и изданиях, рекомендованных Высшей аттестационной комиссией Министерства образования и науки Российской Федерации для опубликования результатов диссертационных исследований:

1. Павлюков В.В. Правовая и практическая возможность объединения данных в информационно-поисковых системах МВД РФ с информацией из сети Интернет / В.В. Павлюков // Вестник Костромского государственного университета имени Н.А. Некрасова. – 2016. – № 3. – С. 226-229. (0,5 п. л.)

2. Павлюков В.В. Компьютерная разведка как оперативно-разыскное мероприятие / В.В. Павлюков // Вестник Нижегородской академии МВД России. – 2016. – № 4 (36). – С.236-241. (0,58 п. л.)

3. Павлюков В.В. Оперативное распознавание лица по фото-, видео- и аудиоданным: перспективы внедрения современных технологий в деятельности органов внутренних дел / В.В. Павлюков // Вестник Костромского государственного университета имени Н.А. Некрасова. – 2016. – № 6. – С. 203-206. (0,5 п. л.)

4. Павлюков В.В. Правовые аспекты получения и защиты компьютерной информации в сети Интернет / В.В. Павлюков // Вестник Дальневосточного юридического института МВД России. – 2017. – № 3 (40). – С. 178-182. (0,58 п. л.)

5. Павлюков В.В. Правовые и организационные основы использования единой информационно-аналитической системы в ОВД / В.В. Павлюков //

Вестник Костромского государственного университета имени Н.А. Некрасова. – 2017. – № 3. – С. 273-275. (0,38 п. л.)

6. Павлюков В.В. Преодоление средств компьютерной защиты как необходимый способ реализации оперативно-разыскного мероприятия «Получение компьютерной информации» / В.В. Павлюков, С.В. Швец // Общество: политика, экономика, право. – 2018. – № 6. [Электронный ресурс] // URL: https://doi.org/10.24158/pep.2018.6.15/ (дата обращения: 20.07.2018). (0,35/0,20 п. л.)

7. Павлюков В.В. Организационно-правовые основы противодействия кибератакам на инфраструктуру государства / В.В. Павлюков // Вестник Московского университета. Серия 11: Право. – 2019. – № 4. – С. 119-128. (0,63 п. л.)

8. Павлюков В.В. Практические способы получения и использования результатов оперативно-розыскного мероприятия «Получение компьютерной информации» / В.В. Павлюков // Вестник Костромского государственного университета. – 2020. – Т. 26. – № 3. – С. 199-203. (0,63 п. л.)

9. Павлюков В.В. Теоретико-правовые основы получения и проверки компьютерной информации, размещённой на сайтах с ограниченным доступом / В.В. Павлюков // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 2 (99). – С. 225-232. (0,81 п. л.)

Статьи в иных изданиях:

1. Павлюков В.В. Некоторые методики раскрытия и расследования преступлений с использованием информационно-поисковых систем ОВД и компьютерной информации из сети Интернет / В.В. Павлюков // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2017. – № 2. – С. 161-173. (0,7 п. л.)

2. Павлюков В.В. Взаимодействие граждан с сотрудниками органов внутренних дел посредством использования компьютерных технологий: состояние и перспективы законодательного обеспечения / В.В. Павлюков // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2021. – № 2 (11). – С. 101-109. (0,58 п. л.)

3. Павлюков В.В. Форма вины преступных деяний, совершенных с помощью мессенджеров / В.В. Павлюков, Д.В. Подтынная // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2022. – № 1 (12). – С. 65-72. (0,21/ 0,31 п. л.)