Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кубанский государственный аграрный университет
имени И.Т. Трубилина»

На правах рукописи

Павлюков Виталий Владимирович

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

5.1.4 Уголовно-правовые науки (юридические науки)

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель
доктор юридических наук, доцент
Швец Сергей Владимирович

Краснодар 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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, 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

---

[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).

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.

ГЛАВА 1. ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

§ 1.1. Понятие и признаки компьютерной информации, используемой в расследовании преступлений

Существующие компьютерные технологии являются современным интеллектуальным потенциалом научной и производственной сферы деятельности человечества, где незаменимым стало получение и анализ компьютерной информации. Компьютерная информация, собранная в единый информационный контур, имеет ряд существенных признаков, которые диаметрально отличают ее от той, которую ранее получали из газет, журналов, книг. В современном обществе постоянно происходит интенсивный перевод всей доступной информации в цифровую форму. Как заявляют отдельные специалисты, на сегодняшний день осталось не оцифрованным чуть более 2% из всего массива существующей информации[1].

Такой технологический рывок стал возможным благодаря тому, что современные компьютеры стали способными не только воспринимать и обрабатывать информацию, представленную в графической форме (текст, в т. ч. рукописный, фотографии, видеоизображения и т. п.), но и управлять компьютерными устройствами с помощью звуковых команд[2], а также анализировать данные при помощи искусственного интеллекта. Информационная сфера – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, требующая адекватного правового регулирования[3].

Для того, чтобы на нормативном уровне четко определить, какую понятийно-терминологическую базу следует использовать в информационной сфере

---

[1] Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 15.

[2] Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. – 2014. – № 1(68). – С. 19.

[3] Рыжов Р.С. Сравнительно-правовой анализ отдельных положений федеральных законов об информации 1995 и 2006 гг // Вестник ВИ МВД России. – 2011. – № 4. – С. 148.; Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – С. 17.

жизнедеятельности российского общества, законодателю придется также сформулировать и четкие ответы по поводу того, что собой представляет феномен компьютерной информации и как последняя (в процессуальном, процедурном, криминалистическом и технологическом плане) может использоваться в правоохранительной деятельности. Правоохранительные органы Российской Федерации лишь тогда станут защитным барьером на пути распространения преступности, когда им по закону будет предоставлена возможность беспрепятственно получать и оперативно использовать компьютерную информацию в целях защиты прав и свобод человека от негативных воздействий в информационной сфере[1].

В спектре обозначенного, считаем целесообразным высказать определенные авторские суждения по поводу того, какими отличительными признаками обладает компьютерная информация и какие связанные с ней понятия могли бы быть взяты за основу при законодательном их закреплении, а также попытаемся обосновать необходимость оперирования данным понятием в целях противодействия преступности.

Начнем с анализа содержания термина «информация», ведь, как правильно заметил С.В. Швец, единого определения информации как научного термина в настоящее время до сих пор не существует[2]. Законодательно такой термин закреплен в ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации»[3]. В этом нормативном акте под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Отдельные ученые тоже солидарны с такой позицией российского законодателя[4].

Но не все правоведы разделяют вышеуказанную точку зрения и предлагают

---

[1] Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. – С. 117.

[2] Швец С.В. Информационные особенности криминалистической деятельности в условиях перевода // Теория и практика общественного развития. – 2014. – № 5. – С. 236.

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.01.2025).

[4] Цимбал В.Н. Понятие, сущность и научное значение криминалистически значимой информации // Вестник КРУ МВД России. – 2010. – № 2. – С. 96.

обращать внимание на то, что информация должна иметь представление и выражаться в определенной форме. Так, Н.В. Ефимкина указывает на то, что информация – это сведения, передаваемые от одного человека к другому, как в письменном виде, так и в устной форме[1].

Е.Р. Россинская и А.И. Семикаленова убеждены, что необходимо изучать в совокупности как особенности создания, хранения и распространения информации в компьютерных системах, так и материальную форму ее хранения и обеспечения возможности ее восприятия[2].

О значимости формы при формулировании понятия «информация» свидетельствует высказывание А.А. Боканова, который разграничивает понятие события, явления, данных, указывая на тот факт, что все это формы информации и что их необходимо различать[3]. По нашему мнению, знания о том, в какой форме будет представлена информация, дает возможность в последствии выявить источник и носитель этой информации, ведь, как указывает Р.С. Белкин, «информация не может существовать без материальной основы, вне информационного сигнала, под которым понимают единство материального носителя и средств передачи информации»[4]. По мнению В.В. Крылова понятия, характеризующие компьютерную информацию требуют детальных пояснений, основанных на понимании как ряда технических характеристик новых средств обработки информации, так и сущности самой компьютерной информации как новой уголовно-правовой и криминалистической категории[5].

Дискуссия по данному факту заставляет нас обратиться к сущности информации, отражение которой зафиксировано в толковом словаре русского языка С.И. Ожегова и Н.Ю. Шведовой интерпретируется как:

---

[1] Ефимкина Н.В. К вопросу об искажении информации в деятельности сотрудников органов внутренних дел // Психопедагогика в правоохранительных органах. – 2013. – № 4(55). – С. 16.

[2] Россинская Е.Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. – 2020. – Т. 11. – № 3. – С.750.

[3] Боканов А.А. Понятие информации в современной экономической науке // Армия и общество. – 2010. – № 1. – С. 125.

[4] Белкин А.Р. Теория доказывания. Научно-методическое пособие. – М.: Издательство НОРМА, 1999. – С. 32.

[5] Крылов В.В. Расследование преступлений в сфере информации. - М.: Издательство «Городец», 1998. – С. 51.

а) сведения об окружающем мире и протекающих в нем процессах, которые воспринимаются человеком или специальным устройством;

б) сообщение, осведомленность о положении дел;

в) совокупность наследственных признаков, которые передаются от клетки к клетке[1].

В связи с тем, что происходит постоянное преобразование информации в компьютерную, назрела необходимость выделить и определить понятие «компьютерная информация». В научной литературе существуют разные подходы как к интерпретации содержания понятия «компьютерная информация», так и к устоявшимся схожими с ней терминами.

Так, действующее российское законодательство содержит определение «компьютерная информация», в примечании 1 к ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Из этого определения следует, что компьютерной информацией является любая информация, которая содержится на электронном материальном носителе. Такие выводы делают А.Ф. Мицкевич и А.В. Суслопаров[2].

Однако в статье 1 ратифицированного РФ «Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164-ФЗ обозначено, что компьютерной информацией должна являться та, которая не только зафиксирована на машинном носителе, но и передаваемая по телекоммуникационным каналам в форме, доступной восприятию электронной вычислительной машине (далее – ЭВМ)[3].

---

[1] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений // Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., дополненное. – М.: ООО «А ТЕМП», 2006. – С. 250.

[2] Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. – 2010. – № 2. – С. 206.

[3] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Федеральный закон от 01 октября 2008 № 164-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 22.02.2025).

А.А. Борисенко указывает на то, что информация всегда предполагает наличие источника и приемника[1], в связи с чем В.С. Пущин, пытаясь расширить понятие и указать на сущность информации, подчеркивает тот факт, что это могут быть любые сведения, представленные в форме, допускающей обмен ими между людьми, человеком и автоматом, автоматом и автоматом[2].

В процессе использования компьютерной информации она может быть преобразована в текстовую, графическую, видео, звуковую, числовую, что существенным образом отличает ее от аналоговой. Это не единственный признак компьютерной информации. Ей присущ еще один признак – неисчерпаемость, а именно, независимо от количества обращений к ней или получения ее копий, она не уменьшается ни в количественном, ни в качественном плане. Таким образом, компьютерная информация быстро стала на вооружение преступности, ведь следы ее хищения нельзя заметить традиционным способом – ее количество у владельца не уменьшается. Здесь необходимо указать, что компьютерная информация копируется на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия средств электросвязи.

Еще одним признаком является то, что при получении компьютерной информации, в отличие от изъятия материального предмета, она сохраняется в первоисточнике.

При работе с информацией, содержащейся в одном файле, доступ к нему одновременно имеют несколько пользователей[3], где возможно обнаружить факт обращения к информации, например, по наличию ее у запрашивающего пользователя. Она будет представлена в виде копии, как правило, на таком же машинном носителе[4].

---

[1] Борисенко А.А. О сущности информации // Фундаментальные исследования. – 2005. – № 7. [Электронный ресурс]. URL: https://www.fundamental-research.ru/ru/article/view?id=6331 (дата обращения: 18.02.2025).

[2] Пущин В.С. Преступления в сфере компьютерной информации. – М., 2000. [Электронный ресурс]. URL: https://ndki.narod.ru/liblary/articles/komp_prest/Puschin_VS-Komp_prest1.doc (дата обращения: 17.06.2024).

[3] Евтеев С.П. Оперативно-розыскное мероприятие «Получение компьютерной информации», Общедоступная информация и информация ограниченного доступа, информационно-телекоммуникационная сеть интернет, осмотр и выемка компьютерной информации // Вестник всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации – 2017. – № 1(41). – С. 47.

[4] Бирюков Д.В. Компьютерная информация как предмет преступного посягательства [Электронный ресурс]. URL: http://aspirantura.16mb.com/doc/conf2015/s3/Biryuk.doc (дата обращения: 20.02.2025).

Несмотря на это, власти развитых стран, где преступления, связанные с использованием компьютерной информации, расследуются многие годы, вынуждены признавать, что выявление таких правонарушений в 90% случаях невозможно[1].

Это связано с признаком обезличенности, а именно, из-за несогласованных и постоянно усовершенствующихся стандартов механизмов работы с компьютерной информацией ее возможно многократно изменять, шифровать, скрыв при этом первоисточник.

Особенностью компьютерной информации является и то, что ее можно получить быстро и в больших объемах, тем самым максимально сократить срок от идеи до преступного результата, и это также обнажает ее общественную опасность[2].

Проблема здесь видится в сложном действующем законодательном механизме регулирования движения компьютерной информации (с данным высказыванием согласились 81% опрошенных нами сотрудников ОВД, при этом 19% высказались против[3]). В п.2 статьи 23 Конституции РФ, четко прописано, что «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения»[4].

Учеными и практиками помимо понятия «компьютерная информация» употребляется также термин «данные». На наш взгляд, обозначенные термины имеют разное смысловое значение. Во избежание путаницы при решении задач ОВД и правового регулирования отношений, связанных с употреблением таких понятий, в данном диссертационном исследовании мы будем исходить из того, что данные термины не являются синонимами и далее приведем отличительные их

---

[1] Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. – 2014. – № 1(31). – С. 115.

[2] Тулегенов В.В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. – 2014. – № 2(33). – С. 96.

[3] См.: Приложение № 1. Опросный лист.

[4] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

признаки.

Возникает также предложение рассмотреть несколько иное понятие, которое бы отражало суть явления. Думается, что такому понятию могла бы соответствовать дефиниция «электронная информация». Однако, если коснуться ее сущности, то П.Г. Смагин приходит к выводу, что особенности такой информации сводятся лишь к ее материальному носителю. Ученый, опираясь на ФЗ «Об информации, информационных технологиях и о защите информации», считает, что не имеет смысла уточнять в законодательных актах форму и вид представления электронной информации, потому что это будет вносить неопределенность в понятие ее сущности и ограничение при ее использовании[1].

Думается, что А.Ф. Мицкевич, возможно, не согласился бы с таким заключением, так как, анализируя различия в понимании информации и данных у нас и за рубежом, он пришел к важному выводу, что, согласно отечественному пониманию компьютерной информации, она может быть определена как вид информации, в то время как, согласно зарубежному пониманию, компьютерная информация является, прежде всего, формой представления информации[2].

Также в зарубежном законодательстве в качестве аналогичного понятия компьютерной информации используются и другие понятия, например: в Польше, Южной Корее – «запись», а в Японии – «электромагнитная запись», в Австралии, Канаде, Финляндии, Германии, Австрии, Голландии – «данные»[3].

Анализируя зарубежный опыт в определении компьютерной информации, З.Н. Индрисова заметила, что «необходимо быть предельно осторожным при использовании терминов «компьютерная информация» и «данные» в международных правовых актах. В разделе, посвященном отличиям между понятиями «информация» и «данные», З.Н. Индрисова отмечает, что подобные различия играют важную роль не только по техническим причинам, но и по

---

[1] Смагин П.Г. О понятии «Компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник ВИ МВД России. – 2008. – № 1. – С. 80.

[2] Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. – 2010. – № 2. – С. 208.

[3] Ястребов Д.А. Понятие, объективные признаки, объект и предмет неправомерного доступа к компьютерной информации. [Электронный ресурс]. – URL: https://superinf.ru/view_helpstud.php?id=478 (дата обращения: 04.02.2025).

причинам верного правового регулирования[1].

Международная организация по стандартизации ISO/IEC обозначает, что данные – это поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, интерпретации или обработки[2].

Здесь стоит заметить, что не все данные стоит называть компьютерной информацией, большинство из них – продукт автоматизированных процессов различных технических устройств (телефонов, компьютеров, навигационных приборов и т. п.), закодированная информация, которую человек не способен понять[3]. Поэтому при использовании термина «данные» с целью его конкретизации не лишним иногда будет говорить «компьютерные данные».

М.Н. Малеина верно указывает на то, что к данным относятся сведения о количестве, времени посещений отдельных сайтов, IP-адрес[4] при использовании физическим лицом по договору с провайдером выделенной линии с фиксированным IP-адресом (поскольку определяется место жительства и место нахождения во время сеанса связи). При этом необходимо сочетание IP-адреса с другими данными для привязки к определенному пользователю[5], из чего следует, что данные – это поддающееся многократной интерпретации представление в формализованном виде и обрабатываемая при помощи компьютерной техники информация. Также данные – это информация, которая хранится, преобразуется и передается при помощи компьютерных систем в цифровом виде и которую человек не способен понять.

Как заметила В.А. Пахомова, отличительным значением любой информации,

---

[1] Индрисова З.Н. Отсутствие законодательного закрепления терминов «Информация» и «Компьютерная информация» как проблема выявления стратегий по борьбе с компьютерной преступностью в Российской федерации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – № 99(5). [Электронный ресурс]. - URL: http://ej.kubagro.ru/2014/05/pdf/88.pdf (дата обращения: 22.01.2025).

[2] ISO/IEC 2382:2015, Information technology – Vocabulary – Part 1: Fundamental terms: a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or communication, or processing [Электронный ресурс]. – URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (дата обращения: 01.02.2025).

[3] Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. – М.: Теис, 1996. – С. 190.

[4] Под IP-адресом стоит понимать уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

[5] Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. – 2010. – № 11(167). – С. 20.

в том числе и компьютерной, является и ее полезность, которая оценивается субъектом, принимающим решение, с точки зрения первичных признаков: релевантности (отнесения сведений к проблемной ситуации) и новизны (способности сведений дополнить знания о проблемной ситуации). Насколько полезна полученная информация покажет способность ее влиять на выбор решения какой-либо определенной проблемы[1].

Именно поэтому получаемая в процессе деятельности ОВД компьютерная информации должна быть сепарирована от той, которая не имеет признаков противоправной деятельности. Так, в юридической литературе преступная деятельность, совершаемая с использованием компьютерной информации, трактуется не однозначно, под ней понимают интернет-преступность, киберпреступность, компьютерную преступность, что требует более детального рассмотрения данных понятий.

Под киберпреступностью О.А. Зигмунт понимает совокупность совершенных на определенной территории за определенный промежуток времени преступных деяний, предметом которых выступают компьютерные сети, компьютерное программное обеспечение, носители компьютерной информации, сетевая информация, а средством совершения являются компьютерная техника либо компьютерные, электронно-информационные технологии[2].

Более широкого понятия киберпреступности придерживается и Д.Н. Карпова, указывая, что киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет[3].

В.А. Номоконов и Т.Л. Тропина приходят к выводу, что киберпреступление – «совокупность преступлений, совершаемых в киберпространстве, с помощью, посредством или против компьютерных систем или компьютерных сетей, а также

---

[1] Пахомова В.А. Понятие термина «Информация» и его историческое развитие // Вестник ЮУрГУ. Серия: Право. – 2013. – № 4. – С. 64.

[2] Зигмунт О.А., Петровский А.В. Кибер и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 181.

[3] Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 47.

иных средств доступа к киберпространству в рамках компьютерных систем или сетей»[1]. Лиц, занимающихся киберпреступлениями, разделяют на хакеров – взломщиков компьютерных систем и сетей; крякеров – взломщиков программного обеспечения; фишеров – создателей поддельных веб-ресурсов с целью получения логина и пароля. Однако, исходя из понятия киберпреступности, невозможно назвать хакером лицо, которое получает информацию из компьютерной сети путем простых запросов в поисковой системе с целью дальнейшего совершения противозаконных действий за пределами компьютерной сети, то есть, использует компьютерную сеть только как источник получения информации, но само преступление совершает в материальном мире.

Поэтому стоит рассмотреть и другое понятие – «компьютерная преступность», которое, как пишет К.И. Попов, традиционно охватывает преступления, совершаемые с помощью компьютеров, информационно-вычислительных систем и средств телекоммуникаций или направленные против них с корыстными либо некоторыми другими целями[2].

Некоторые авторы полагают, что неправильно говорить – преступление совершается с помощью компьютера. Так, например, М.А. Простосердов подчеркивает, что под такие действия «могут попадать и преступления, в которых компьютер был применён не по своему основному назначению, например, в случае если компьютером был нанесён удар другому человеку»[3].

В связи с тем, что преступления в сфере компьютерной информации продолжают развиваться, расширяются возможности, совершенствуются орудия и средства их совершения, возникают новые и видоизменяются старые способы совершения преступлений[4]. Поэтому стоит указать, что, если раньше компьютерная информация использовалась с целью выявления преступлений,

---

[1] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 48.

[2] Попов К.И. Компьютерные преступления – преступления мирового масштаба // Правопорядок: история, теория, практика. – 2013. – № 1(1). – С. 28.

[3] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – М., 2016. – С. 26.

[4] Махтаев М.Ш., Лебедь И.Е. Криминалистические аспекты предупреждения преступлений в сфере компьютерной информации // Вестник Российского нового университета. Серия: Человек и общество. – 2009. – № 4. – С. 29.

совершаемых хакерами с целью получения удаленного доступа, уничтожения, модификации, блокирования, шифрования информации на компьютерных устройствах, то сейчас она все чаще имеет значение при выявлении преступлений, которые совершаются в отношении обычных пользователей.

Стоит согласиться с Н.Л. Коликовым, который заметил, что профессиональная компьютерная преступность входит в состав общей преступности, ее криминогенность создает условия для совершения других преступлений, не относящихся к компьютерной преступности.

Также в числе тенденций преступлений, совершаемых при помощи компьютерной информации, все большее число «традиционных» составов преступлений, постепенно перемещаются в сферу компьютеров и их систем[1]. Это, например, обуславливается тем, что компьютерная информация, находящаяся в открытом доступе в сети Интернет, может содержать сведения об устройстве и создании взрывчатых, наркотических веществ, об изготовлении в домашних условиях огнестрельного оружия и т. д.[2].

На этом также акцентирует свое внимание О.Ю. Введенская, по собранным статистическим данным которой компьютерная информация принята на вооружение преступниками любых категорий, являясь не только способом (30%), но и средством совершения «традиционных» преступлений (46% – средство подготовки преступлений, 24 % – средство их сокрытия), выходя таким образом за ранее обозначенные рамки[3].

Анализ законодательной базы и вышеуказанных статистических данных заставляет указать на две тенденции, а именно:

первая тенденция – преступления, совершаемые при помощи компьютерной информации с целью получения удаленного доступа, уничтожения, модификации, блокирования, шифрования информации на компьютерных устройствах, ученые в

---

[1] Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. ... д-ра юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. – Москва. – 2016. – С. 8.

[2] Коликов Н.Л. Причины и условия профессиональной компьютерной преступности // Вестник ЮУрГУ. Серия: Право. – 2011. – № 19(236). – С. 32.

[3] Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 210.

большинстве случаев называют «киберпреступлениями», к таким относят те, которые указаны в ст. 159.6. и в статьях главы 28 УК РФ[1];

вторая тенденция – преступления, совершаемые при помощи компьютерной информации, компьютерных систем именуют «компьютерные преступления», к последним можно отнести большинство тех, которые совершаются в реальном мире в отношении людей, где факт их совершения был запечатлен при помощи компьютера или компьютерная информация послужила средством для их совершения.

С позиций совершенствования законодательства и правоприменительной практики Российского государства более предпочтительным выглядит развитие второй тенденции – то есть оперирование термином «компьютерные преступления». Что касается понятия киберпреступности, то его следовало бы использовать только в научных исследованиях и то лишь в качестве синонима компьютерных преступлений. Поэтому в своем диссертационном исследовании мы попытаемся оперировать в основном понятийным рядом: «компьютерные преступления» – «компьютерная преступность», заменяя его лишь иногда соответствующими синонимами. Более того, при характеристике компьютерных преступлений, мы будем руководствоваться тем, что создание, сохранение, передача, обработка и анализ компьютерной информации оперативно-розыскного значения возможны только при помощи компьютерной техники, посредством преобразования ее с использованием двоичных кодов.

Чтобы иметь полное представление о феноменах «компьютерные преступления» и «компьютерная преступность», следует ответить еще на один очень важный вопрос – какая компьютерная техника может использоваться в целях незаконного получения компьютерной информации?

А.В. Касаткин структурирует использование компьютерной техники и программного обеспечения в преступных целях в следующих формах:

---

[1] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук: 12.00.12 / Шевченко Елизавета Сергеевна. – Москва, 2016. – С. 26; Гришин Ю.В., Иванов А.В., Карпова Н.Е., Чуваков А.В. Применение автоматизированных систем в компьютерной криминалистике // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 25.

- использование программных продуктов в качестве объекта преступления (незаконное копирование, причинение ущерба применением разрушающих программ – вирусов);

-использование программных продуктов в качестве инструмента совершения преступления (несанкционированное проникновение в компьютерную систему, искажения и подлоги информации);

-объектом совершения преступления являются технические средства ЭВМ (кража компьютера, незаконное использование машинного времени);

-использование технических средств ЭВМ как средства совершения преступления (внесение изменений в информационную базу, изготовление с помощью печатной базы ЭВМ фальшивых документов) [1].

Становится очевидным, что умелое использование технических средств и программного обеспечения должно выступать не только в пользу злоумышленника, но и стать основным средством получения компьютерной информации о противоправной деятельности подразделениями ОВД. Компьютерную информацию, как и информацию в целом, содержащую сведения о совершаемом преступлении, называют криминалистически значимой информацией или информацией, имеющей значение в расследовании преступлений оперативно-розыскного значения или оперативно-розыскной информацией (далее – ОРИ), которая также имеет отличительные признаки. Как отмечает С.С. Овчинский, от иной социальной информации «ОРИ отличают цель получения (борьба с преступностью), методы получения и режим использования, обеспечивающие конспирацию, надежную зашифровку источников, возможность проверки сообщаемых сведений и их применения только заинтересованными оперативными и следственными аппаратами».

ОРИ содержит сведения о причинной связи между событиями и фактами, анализ и оценка которых ведет к установлению обстоятельств преступления, круга соучастников[2]. Она содержит знания о событиях, которые свидетельствуют о

[1] Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / Касаткин Андрей Валерьевич. – М., 1997. – С 17.

[2] Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского,

преступной деятельности конкретных лиц, раскрывает механизм совершенного преступления или того, что готовится. ОРИ отражает результаты негласной фиксации конкретных действий лиц, подозреваемых или разрабатываемых ОВД, дает возможность целенаправленно контролировать их преступные действия. Это определяет ее значимость в процессе доказывания по уголовному делу, обеспечивая при этом следователю и суду возможность непосредственного восприятия реальных фактов преступной деятельности.

При этом следует помнить, что ОРИ с точки зрения ее содержания «... отражает не только те явления, события, происшествия, изменения в среде, которые возникают в результате преступлений, но и широкий круг явлений, обстоятельств, событий, влияющих на преступность в целом и на преступное поведение отдельных лиц»[1]. Многие экономические, политические, демографические и другие социальные процессы, рассматриваемые в связи с борьбой с преступностью, приобретают характер ОРИ.

До принятия ФЗ «Об оперативно-розыскной деятельности» некоторые исследователи определяли ОРИ как «... получаемые в результате обнаружения, сбора, обработки, анализа и оценки фактических информационных данных сведения о замышляемых, подготавливаемых и совершенных преступлениях, о лицах, представляющих оперативный интерес, о разыскиваемых преступниках, об обстоятельствах, имеющих значение для планирования и осуществления оперативно-розыскных мероприятий и оперативно-аналитической работы, а также оказания содействия предварительному расследованию»[2].

Ранее такое же определение было высказано В.А. Лукашовым в полемике с Д.В. Гребельским[3]. Оно является в целом верным, но, на наш взгляд, не учитывает специфики возникновения ОРИ как результата деятельности оперативных подразделений с использованием средств и методов ОРД.

Г.К. Синилова. М.: ИНФРА-М, 2006. – С. 621.

[1] См.: Там же. – С. 9.

[2] Оперативно-розыскная деятельность органов внутренних дел. Термины и определения: Учеб, пособие / Под ред. Ю.И. Римаренко. – Киев: НИиРИО КВШ МВД СССР, 1988. – С. 145-146.

[3] Лукашов В.А. О сущности и значении оперативно-розыскной информации // Информационное сообщение лаборатории проблем оперативно- розыскной работы. – М.: НИиРИО ВШ МВД СССР, 1973. – № 3. – С. 21-22.

Как справедливо отметил И.П. Козаченко, «решающее, что раскрывает специфическое оперативно-розыскное содержание информации – это особенности самой сущности ОРД, ее принципов, характера возникающих отношений при получении, оценке и использовании информации, профессиональных свойств субъектов, участвующих в информационном обеспечении ОРД. Отсюда вытекает и специфика получения ОРИ, которая по самому своему происхождению в большинстве случаев является результатом применения негласных сил, средств и методов ОРД либо гласно полученной и проверенной негласным путем»[1].

М.В. Маркелов и В.Ю. Фролов предъявляют следующие основные требования к ОРИ: вероятность, полнота, своевременность, непрерывность и систематичность поступления[2]. П.Ф. Телепнев указывает, что оперативно-розыскная информация должна быть зафиксирована в соответствии с требованиями нормативных правовых актов, которые используются для решения задач, определенных ФЗ «Об оперативно-розыскной деятельности», а также для обеспечения уголовного судопроизводства[3]. Стоит добавить, что информация оперативно-розыскного значения должна быть достоверная и проверена оперативным сотрудником. Обозначенные требования, из которых вытекают и признаки информации оперативно-розыскного значения, на наш взгляд, являются исчерпывающими и должны быть применимы, в том числе, к компьютерной информации, используемой в расследовании преступлений в целом.

М.В. Кремлев, анализируя понятие информации, используемой в ходе расследования преступлений, считает, что «Под таковой следует понимать данные в виде сигналов, преобразованных мыслительной деятельностью следователя и преломленных субъективными факторами, снимающими неопределенность»[4]. Как

---

[1] Козаченко И.П. К вопросу об информационном обеспечении оперативно-розыскной деятельности органов внутренних дел // Актуальные вопросы получения, оценки и использования информации в оперативно-розыскной деятельности органов внутренних дел. – Киев: НИиРИО КВШ МВД СССР, 1986. – С. 5.

[2] Маркелов М.В., Фролов В.Ю. Основные элементы организации оперативно-розыскной деятельности органов внутренних дел // Актуальные проблемы теории оперативно-розыскной деятельности. – Омск: НИиРИО Омской ВШ МВД СССР, 1986. – С. 97-98.

[3] Телепнев П.Ф. Научный взгляд на определение понятия оперативно-розыскной информации // Вестник Санкт-Петербургского университета МВД России, 2016. – № 1 (69). – С. 139.

[4] Кремлев М.В. К вопросу о понятии информации, используемой в ходе расследования преступлений // Человек: преступление и наказание. – 2014. – № 4 (87). – С.103.

и любая другая информация, компьютерная информация существенно влияет на процесс раскрытия, расследования и предупреждения преступлений. Данная деятельность осуществляется, в первую очередь, специально уполномоченными на то субъектами ОВД и направлена на поиск сведений, с помощью которых возможно получение значимой в расследовании информации с целью выявления, предупреждения, пресечения и раскрытия преступлений, а также розыска, выявления и установления лиц, их подготавливающих, совершающих или совершивших[1].

Определяя понятие компьютерной информации в расследовании преступлений, стоит указать, что таковая может быть получена как уполномоченными на то сотрудниками оперативных подразделений с применением оперативно-розыскных мероприятий, так и следователями при проведении следственных действий.

Не менее важным для более углубленного понимания формы проявления, содержания и особенностей использования компьютерной информации в расследовании преступлений является также осуществление классификации такой информации. И в этом ракурсе мы обратим внимание, прежде всего, на Директиву 2006/24/ЕС «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования» (далее – «Директива 2006/24/ЕС»), где ключевое значение имеют нормативные положения ст. 5, согласно которой компьютерная информация, используемая в расследовании преступлений, классифицирована по категориям, в соответствии с которыми необходимо производить обнаружение и идентификацию источника сообщения; адресата коммуникации; даты, времени, длительности; типа коммуникации и коммуникационного оборудования; местоположения оборудования мобильной связи[2].

---

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп.) [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[2] Directive 2006/24/EC of the European parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Электронный ресурс]. – URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (дата обращения: 15.02.2025).

Считаем, что не лишним будет здесь добавить еще одну категорию, которая позволяла бы зафиксировать активность передачи данных в компьютерной сети, а именно объем отправленных и полученных данных за определенный промежуток времени на конкретный ресурс с целью идентификации активности пользователя, например, на ресурсах сети Интернет. Соответственно, можно выделить еще один признак компьютерной информации, а именно, измерение ее в объеме (байт).

Резюмируя изложенное, еще раз акцентируем внимание на том, что в условиях стремительного научно-технического прогресса успешное решение задач борьбы с преступностью невозможно без оптимизации процессов применения и использования компьютерной информации в повседневной работе подразделений ОВД. Роль компьютерной информации, используемой в расследовании преступлений, полученной техническими средствами, пропорциональна использованию совершаемых при помощи нее преступлений. Субъекты, которые задумают произвести кибератаку, смогут остаться незамеченными, указав ложный след, приводящий к тому государству, которое не совершало данное деяние[1].

Правовые механизмы получения и использования компьютерной информации должны постоянно совершенствоваться. Поэтому, чтобы правоохранительные органы Российской Федерации имели реальную возможность использовать компьютерную информацию в целях эффективного решения поставленных задач, с учетом вышеизложенного стоит разграничить компьютерную информацию по следующим признакам:

- трансграничность: компьютерная информация пересылается на любые расстояния, ограниченные только радиусом действия средств электросвязи;

- относительная неисчерпаемость: независимо от количества обращений к компьютерной информации или получения ее копий, она не уменьшается ни в количественном, ни в качественном плане и остается в первоисточнике;

- измеримость: компьютерная информация измеряется в битах;

- трансформируемость: информация может быть изменена и преобразована в

[1] Саенко С.И., Павлюков В.В. Правовые, организационные и технологические способы обеспечения кибербезопасности на земле и в космосе // Охрана, безопасность, связь. – 2023. - № 8-1. – С. 103.

текстовую, графическую, видео, звуковую, числовую, что позволяет получать новые формы и представления (например, через редактирование, конвертацию форматов);

доступность: компьютерная информация может быть получена, скопирована и передана в любое время и из любого места при наличии интернет-соединения. С одним источником, содержащим компьютерную информацию может одновременно работать несколько пользователей. С компьютерной информацией возможно взаимодействовать через различные технические и программные средства. При помощи программного обеспечения становится доступным структурировать компьютерную информацию в различные форматы. Компьютерную информацию возможно копировать на различные виды машинных носителей (накопитель на жёстком магнитном диске (HDD), твердотельные накопители (SSD), флэш – накопители, и других);

защищенность: компьютерная информация может быть защищена несколькими уровнями: физически - путем ограничения физического доступа к источнику, на котором хранится информация; технически (аппаратно) при помощи физических устройств и приборов аутентификации и идентификации пользователей, а также аппаратных межсетевых экранов и шифраторов каналов связи; программно, а именно при помощи встроенных функций безопасности в операционную систему, а также специализированного программного обеспечения (далее – ПО) (антивирусное ПО, системы идентификации, аутентификации пользователей и разграничения доступа, программы шифрования данных, системы обнаружения и предотвращения вторжений, программы анализа контроля действий пользователей, системы резервного копирования и восстановления данных);

обезличенность: из-за постоянно усовершенствующихся стандартов и механизмов работы с компьютерной информацией ее возможно многократно изменять, шифровать, подменять адрес отправителя, скрыв при этом первоисточник;

автоматизация обработки: компьютерные устройства способны

автоматически выполнять операции с информацией, что позволяет ускорять обработку данных и снижать вероятность ошибок, а также позволяют анализировать большие объемы информации.

С учетом имеющихся признаков необходимо на законодательном уровне четко зафиксировать в одном нормативно-правовом акте, а именно в ФЗ «Об информации, информационных технологиях и о защите информации», следующие понятия: «информация», «компьютерная информация» и «компьютерная информация, используемая в расследовании преступлений».

На наш взгляд, возможно нормативное закрепление следующих дефиниций:

1) **информация** – это любые сведения, знания, сигналы, данные, полученные в процессе их познания непосредственно человеком, либо с использованием научно-технических средств, которые в дальнейшем могут быть зафиксированы в памяти человека или отображены и храниться при помощи искусственного языка на материальном носителе, где, в зависимости от формы предоставления, позволяют производить различные манипуляции;

2) **компьютерная информация** – совокупность цифровых данных, имеющих различную форму представления (текстовую, графическую, видео, звуковую, числовую), находящихся на электронных носителях, которые могут быть получены, сохранены, отображены, изменены, закодированы с возможностью дальнейшей передачи при помощи компьютерных устройств и систем в виде электронных, световых, звуковых или радиосигналов;

3) **компьютерная информация, используемая в расследовании преступлений** – совокупность актуальных данных, находящихся в компьютере, на компьютерных носителях или передаваемых при помощи компьютерных сетей и систем, имеющих криминалистическое 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.

§ 1.2. Источники компьютерной информации, используемой в расследовании преступлений

Потребность сотрудников ОВД в информации неразрывно связана с поиском её источников и фиксации содержащихся в них сведений, указывающих на признаки противоправной деятельности.

Деятельность правоохранительных органов по раскрытию и расследованию преступлений начинается со сбора информации о случившемся, с поиска следов и сведений о совершенном преступлении, подчеркивает Г.А. Погосян[1].

Анализ оперативной и следственной практики показывает, что наиболее доступным и быстро развивающимся открытым источником информации в настоящее время является сфера информационных технологий. В последней каждый может получать доступ к безграничному объему компьютерной информации, используя различное программное обеспечение, установленное на технические средства связи, будь то персональный стационарный компьютер или мобильный телефон, что было адаптировано и принято преступной средой как система методов по подготовке, совершению и сокрытию преступлений[2].

Актуальность такого информационного ресурса совпадает с современными потребностями, ведь именно в компьютерной сети накоплена и зафиксирована на материальных носителях информация об окружающей нас действительности[3], с которой возможно работать дистанционно.

При помощи компьютерных сетей и систем возможно производить поиск компьютерной информации различного характера, однако, необходимо проанализировать и выявить такие источники информации, которые могут предоставить сведения для выдвижения версий о противоправной деятельности.

---

[1] Погосян Г.А. Проблемы получения и использования криминалистически значимой информации в качестве доказательств на предварительном следствии: Процессуальные и криминалистические аспекты дис. канд. юрид. наук: 12.00.09. – Краснодар, 2006. – С. 105.

[2] Бахтеев Д.В. О некоторых способах сокрытия и обнаружения компьютерной информации // Сборник материалов криминалистических чтений. – 2017. – № 14. – С. 18.

[3] Ткалич В.Л., Лабковская Р.Я., Пирожникова О.И., Коробейников А.Г., Симоненко З.Г., Монахов Ю.С. Патентоведение и защита интеллектуальной собственности. / Учебное пособие. – СПб: Университет ИТМО, 2015. – С. 12.

Стоит указать, что при помощи компьютерных устройств и сетей вполне реально получать сведения в виде компьютерной информации о лицах, событиях и обстоятельствах совершения преступлений, которые открывают новые возможности для органов внутренних дел, действуя в условиях анонимности, что во многом облегчает зашифровку применяемых сил, средств и методов[1].

В.А. Родивилина полагает, что сейчас не имеет никакого смысла то, чем и на чем записана информация. Главное, по мнению автора, – это уметь получать компьютерную информацию и знать, какая информация записана, как можно ее воспроизвести, проверить, оценить и сохранить необходимое время с помощью технических средств, имеющихся в распоряжении сотрудников ОВД[2].

Не смотря на сложный механизм поиска противоправных действий, совершаемых при помощи компьютерных технологий, Р.В. Нагорняк считает, что память компьютера содержит электронные следы, выявление и исследование которых также возможно наряду со следами материальными и это должно занимать центральное место при раскрытии и расследовании преступлений, совершенных при помощи сети Интернет[3].

Сложность в изучении и анализе исследуемого вопроса обусловлена, кроме всего прочего, отсутствием единой общепринятой устоявшейся терминологии. Так, например, компьютерная система с циркулирующей в ней информацией имеет ряд схожих, однако до сих пор не утвердившихся названий: «кибер» или «виртуальное» пространство.

Проанализировав работы ряда ученых, М.А. Простосердов приходит к выводу, что киберпространство – это искусственно созданная среда, существование которой ограничено информационно-телекоммуникационной сетью, пользователи

---

[1] Евтеев С.П. Оперативно-розыскное мероприятие «Получение компьютерной информации», Общедоступная информация и информация ограниченного доступа, информационно-телекоммуникационная сеть интернет, осмотр и выемка компьютерной информации // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2017. – № 1(41). – С. 43.

[2] Родивилина В.А. Процессуальные особенности использования технических средств в стадии предварительного расследования дис. ... канд. юрид. наук / Родивилина Виктория Александровна. – Иркутск, 2016. – С. 50.

[3] Нагорняк Р.В. Получение компьютерной информации: содержание и разграничение с другими оперативно-розыскными мероприятиями // Сборник материалов Всероссийской научно-практической конференции молодых учёных / Современность в творчестве начинающего исследователя. – 2017. – С. 161.

которой могут свободно вступать в административные, гражданские, уголовные и другие правоотношения[1].

Есть и другая точка зрения, высказанная А.В. Нестеровым, который указывает, что киберпространство – это свойство виртуального поля, которое может продуцироваться в инфраструктуре Интернета. Поэтому люди взаимодействуют с помощью элементов виртуального интернет-поля, а не киберпространства. В этой связи слово «киберпространство» можно считать метафорой. Мы же согласны с высказыванием А.В. Нестерова, который подчеркивает, что обозначать интернет-поле как киберпространство нельзя, т.к. понятие пространства обозначает свойство поля, а не само поле, в том числе и виртуальное[2].

Закономерно возникает вопрос об употреблении понятия «киберпространство» в законодательстве, где, по нашему мнению, для общего понимания данный термин возможно оставить, хотя этот термин обозначает ту долю компьютерной сети Интернет, которая включает в себя виртуальное пространство, но не затрагивает технические аспекты взаимодействия компьютеров в сети.

Поэтому в дальнейшем исследовании, чтобы избежать путаницы, будет употребляться термин «компьютерная сеть», под которой следует понимать объединенные между собой при помощи проводных и беспроводных технологий, а также различных технических маршрутизирующих устройств (роутеры, маршрутизаторы, компьютеры с несколькими сетевыми картами, сервер маршрутизации) два и более компьютерных устройства, которые взаимодействуют по единым правилам с целью получения доступа и использования различных сервисов, информационных ресурсов, программ и периферийных устройств.

Стоит сразу оговориться и обозначить отличия компьютерной сети от компьютерной системы. Так, компьютерная система работает поверх компьютерной сети и представляет собой совокупность аппаратных средств, управляемых при помощи программного обеспечения. Компьютерная система

---

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис.... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – М., 2016. – С. 22.

[2] Нестеров А.В. Интернет-поле VS киберпространства // Вопросы безопасности. – 2015. – № 4. – С. 15.

может также предоставлять общие услуги, такие как управление доступом, взаимодействие процессоров и графический интерфейс пользователя.

При помощи компьютерных систем пользователи могут быстро получать информацию и обмениваться ею, оставлять данные о себе и своей деятельности, задавать вопросы и подвергать критике мысли и убеждения других людей, все чаще воспринимая при этом происходящее в виртуальном мире как реальное. В.А. Сокольникова точно подмечает, что сегодня Интернет влияет на жизнедеятельность многих людей гораздо сильнее, чем физический (материальный) мир[1].

Как показывает практика, более сложные преступления в сфере информационных технологий совершаются с использованием возможностей компьютерных устройств с выходом в Интернет. К основным средствам передачи информации и одновременно орудиям механизма преступной деятельности О.С. Кучин справедливо относит современные мобильные телефоны, устройства доступа к ресурсам сети Интернет, а также радиостанции[2].

«Компьютерная преступность – объективное следствие происходящей глобализации информационных процессов», сетуют С.Я. Казанцев и О.Э. Згадзай. По их суждению, постоянно происходит усложнение и видоизменение преступной деятельности, связанной с использованием глобальных компьютерных сетей, и нет никаких оснований считать, что в ближайшее время ситуация может измениться в лучшую сторону[3].

Криминальная статистика, отраженная на сайте Генеральной прокуратуры Российской Федерации, свидетельствует о том, что количество противоправных деяний, совершаемых с использованием информационных технологий в России, постоянно растет. За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до

---

[1] Сокольникова В.А. Информация и информационно-коммуникативные технологии (ИТ) в эпоху современной глобализации // Пробелы в российском законодательстве. – 2014. – № 6. – С. 290.

[2] Кучин О.С. Средства и орудия как элемент механизма преступной деятельности экстремистского характера // Известия Тульского государственного университета. экономические и юридические науки. – 2017. – № 4-2. – С. 49.

[3] Казанцев С.Я., Згадзай О.Э. Экономическая преступность в IT-сфере. Новые угрозы и необходимые ответы // Вестник Казанского юридического института МВД России. – 2011. – № 3. – С. 31.

25 %[1]. На конец 2024 года показатели киберпреступности остаются на высоком уровне.

Считаем, что это не полная картина происходящего, так как, выявив преступление или будучи его жертвой, лица, которые понесли материальный или иной ущерб, часто не обращаются в правоохранительные органы, что, по мнению А.А. Скурихиной и О.С. Ронжина, обусловлено следующими факторами:

- неверие граждан в возможный положительный исход их обращения в правоохранительные органы;

- нежелание предавать огласке сведения, порочащие самого пользователя и т. п.

Ученые отмечают, что в большинстве случаев жертвы компьютерных преступлений не подозревают о том, что являются потерпевшими. Они не в состоянии обнаружить факт совершения в отношении них преступления, если не наступают материальные последствия[2], а если им даже и становится известен факт совершения преступления, то источник этого правонарушения остается неизвестен.

Поэтому рассмотрение вопроса о возможности использования информации в расследовании преступлений следует начать с определения понятия источников такой информации. В связи с этим можно поддержать позицию М.Х. Иванова, который в качестве источников рассматривает лиц, материальные объекты, системы, которые сообщают или содержат данные о совершенных преступлениях или таких, которые задумываются или готовятся[3].

Следы, в том числе имеющие значение в расследовании преступлений, учёные криминалисты традиционно подразделяют на «материальные» и «идеальные»[4]. К

---

[1] Портал правовой статистики [Электронный ресурс] // Генеральная прокуратура Российской Федерации. – URL: http://crimestat.ru/analytics (дата обращения: 01.02.2025).

[2] Скурихина А.А., Ронжина О.С. Виктимность в сфере компьютерных преступлений // Виктимология. – 2014. – № 2(2). – С. 49.

[3] Оперативно-розыскная деятельность органов внутренних дел. Термины и определения: Учеб, пособие / Под ред. Ю.И. Римаренко. - Киев: НИиРИО КВШ МВД СССР, 1988. – С. 146.

[4] Суворова Л.А. Идеальные следы в криминалистике: Дис. … канд. юрид. наук: 12.00.09 / Суворова Людмила Александровна. – Воронеж, 2005. – 245 с.; Хорунжий С.Н. Следы в криминалистике и особенности их выявления и использования при расследовании групповых преступлений: Дис. … канд. юрид. наук: 12.00.09 / Хорунжий Сергей Николаевич. – Воронеж, 2001. – 224 с.; Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: Дис. … канд. юрид. наук: 12.00.09 / Лыткин Николай

источникам идеальных следов относятся негласные сотрудники, граждане, представители общественности, должностные лица и т. д. К материальным следам относятся материалы, полученные в результате применения сил, средств и методов ОРД, оперативно-розыскные и криминалистические учеты, материалы уголовных дел, материалы других служб ОВД, материалы юридических лиц и т. д.

Среди источников информации, используемой в расследовании преступлений, могут преобладать «идеальные», то есть субъекты-носители информации. При этом наиболее ценными источниками можно считать агентов, доверенных лиц, резидентов, держателей конспиративных, явочных квартир и явочных мест, внештатных работников оперативных подразделений, очевидцев, свидетелей.

Примечательно, что информация, используемая в расследовании преступлений, полученная от «идеальных» следов, имеет тенденцию к искажению на этапах ее получения и передачи оперативному работнику, каждый из участников коммуникационного процесса одни и те же понятия может толковать по-разному[1], что обусловлено субъективизмом в восприятии информации источником, оценке информации источником и особенностями передачи информации языковыми средствами.

Субъективизм восприятия информации объясняется тем, что человек, который получает информацию, в силу особенностей психики всегда придает ей эмоциональную окраску в зависимости от своего положения в обществе, уровня образованности, темперамента, наличия связей с преступниками, личной заинтересованности в результатах передачи информации оперативному работнику. Оценка информации источником заключается в индивидуальном разделении событий на главные и второстепенные, основные и неосновные, значимые и незначительные, важные и неважные и приводит к выпадению из сообщения необходимых деталей, которые играют иногда определяющую, ключевую роль.

Искажение информации происходит также на этапах ее восприятия и передачи сотруднику ОВД по причине несовместимости языково-логических конструкций.

Николаевич. – М., 2007. – 201 с.

[1] Швец С.В. Методические вопросы судебно-лингвистической экспертизы // Судебная экспертиза. – 2008. – № 1. – С. 92.

Люди, проживающие на различных территориях, отличающиеся по социальному статусу, уровню интеллекта, образованию, национальности, возрасту, профессии, – используют различные диалекты, сленг, а также свой понятийный аппарат.

Указанные особенности информации, полученной от «идеальных» источников, негативно сказываются на ее достоверности, полноте, точности и лаконичности.

Этих недостатков лишена информация, полученная из «материальных» источников, поскольку сотрудник ОВД получает ее непосредственно из материального мира, минуя субъективного посредника. Такая информация объективна по своей природе, она поступает к потребителю в неискаженном виде и поэтому всегда имеет максимально возможную в данных условиях полноту. По мере развития компьютерных технологий точность информации, получаемой при помощи технических средств, постоянно растет.

Информация, полученная от «материальных» источников, всегда лаконична, поскольку отсутствует дополнительное звено ее передачи – субъективный посредник, который может являться источником лишних сведений для расследования.

Таким образом, информация, полученная из «материальных» источников, всегда может быть правильно воспринятой сотрудником ОВД и служит основой для выдвижения версий и принятия верного решения при проведении оперативно-розыскных мероприятий, следственных и других действий.

В случае получения компьютерной информации при помощи технических средств в качестве ее «материальных» источников могут выступать различные носители информации (накопитель на жёстких магнитных дисках HDD, твердотельные накопители SSD, флеш-накопители, мобильные телефоны, видеорегистраторы и т. д.).

В связи с тем, что благодаря современным компьютерным системам происходит постоянное увеличение информационных потоков, их стоит рассматривать не только как технологические информационные системы, но и как инструменты для информационного поиска, а также в качестве первоочередных

источников компьютерной информации, которая может быть использована в расследовании.

Следует отметить, что отдельными авторами, например. А.Л. Осипенко, уже акцентировано внимание на необходимости ОВД признавать в качестве перспективных следующие источники получения компьютерной информации:

- устройства и технические средства, которые могут содержать сведения о разрабатываемых лицах (компьютерная техника, средства сотовой связи и мобильные устройства);

- различные носители компьютерной информации, служащие для хранения данных, которые могут представлять оперативный интерес (специальные устройства, оснащенные различными датчиками, такими как GPS/ГЛОНАС-трекеры, фиксирующие местоположение, электронные RFID ключи, позволяющие провести идентификацию устройства);

- устройства, оснащенные нательными измерителями, фиксирующими различные физиологические данные;

- устройства аудио-видео фиксации;

- средства, обеспечивающие доступ к сетевым ресурсам[1].

Научное обоснование целесообразности использования в ОВД определенных источников компьютерной информации, указывающей на признаки противоправной деятельности того или иного лица, должно и дальше продолжаться. И в этом направлении видится перспективным выделение данных источников на основе изучения способов совершения компьютерных преступлений.

О.Н. Скоморохов и Е.В. Чиненов подчеркивают, что способ совершения является важнейшим элементом криминалистической характеристики преступления. Изучение способа совершения преступления занимает одно из центральных мест в криминалистике и обеспечивает успешное решение ряда поисковых задач[2].

---

[1] Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. – 2016. – № 3. – С. 86.

[2] Скоморохов О.Н., Чиненов Е.В. Особенности криминалистической характеристики заведомо ложного

Если рассматривать информационно-телекоммуникационные сети как среду совершения различных форм противоправных действий, например, кражи, то предметом преступного посягательства могут быть персональные данные, денежные средства и иное имущество, например, в случае использования сети Интернет при снятии денежных средств с похищенной банковской карты. В этом случае в качестве источника информации могут быть электронные кошельки, сведения о движении денежных средств в различных финансовых организациях, а также сервисах обмена валют. Можно согласиться с Н.В. Летёлкиным, который указывает, что использование компьютерных систем служит также средством для совершения таких деяний, как: клевета, шпионаж, экономический шпионаж, сексуальное домогательство, ряд преступлений, посягающих на компьютерную информацию, продажа оружия, продажа алкогольной продукции, мошенничество с ценными бумагами, распространение наркотических средств, преступления против половой свободы и неприкосновенности несовершеннолетних, распространение детской порнографии[1]. Возможности сети Интернет способствуют распространению информации об изготовлении и продаже опасных психотропных веществ[2]. Для этих целей злоумышленники используют как готовые сайты, социальные сети, так и создают специализированные интернет-ресурсы. Стоит привести в пример сайт «Silk Road», деятельность которого началась в 2011 году. Одно из главных условий в работе сайта было сочетание технологии анонимного доступа к ресурсу через браузер Tor и анонимной оплаты товара с помощью криптовалюты Bitcoin. Необходимость в этих ухищрениях была обусловлена тем, что большинство товаров на торговой площадке «Silk Road» были полностью незаконными или не совсем законными. Так, при помощи сайта «Silk Road» возможно было приобрести не только наркотики, оружие, но и даже

сообщения об акте терроризма посредством сети Интернет // Проблемы правоохранительной деятельности. – 2013. – № 1. – С. 62.

[1] Летёлкин Н.В. Особенности уголовно-правового противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») в законодательстве стран англосаксонской правовой семьи (на примере Великобритании и США) // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 2(34). – С. 307.

[2] Решняк О.А. Расследование преступлений в сфере незаконного сбыта опасных психотропных веществ, совершенных с использованием компьютерных технологий : монография / О.А. Решняк, С.А. Ковалев, В.Б. Вехов. – Волгоград : ВА МВД России, 2020. – С.28.

заказать киллера[1].

Однако обычному обывателю будет весьма сложно объяснить механизм работы Tor - браузера, а тем более способы пополнения и перевода криптовалюты между криптокошельками. Очевидно, что намного легче осуществить перевод между обычными банковскими счетами. В свой черед, банки, по запросу от правоохранительных органов, могут указать на лицо, причастное к противоправной деятельности. В связи с этим в поисках путей получения денежных средств некоторые злоумышленники довольно успешно начали использовать посредников в своей деятельности, или людей, которых называют «Дропами» (от английского «drops», что переводится как «сбросы»), а именно лиц, которые соглашаются принять на себя ответственность за преступные действия, часто не осознавая полного масштаба совершаемых преступлений. Преступления с использованием дропов могут принимать различные формы. К таким можно отнести:

Финансовые мошенничества:

1. Использование дропов для получения кредитов, займов или других финансовых услуг на подставные имена, открытие банковских счетов на дропов для отмывания денег.

2. Интернет-мошенничество: создание дропов для получения товаров, купленных с использованием украденных кредитных карт или мошеннических схем, использование дропов для регистрации аккаунтов на платформах, что дает возможность осуществлять преступные действия анонимно.

3. Наркоторговля: привлечение дропов для получения и распространения наркотиков, чтобы минимизировать риск ареста для настоящих участников.

4. Кража личных данных: дропы могут использоваться для получения и хранения украденной информации, что затрудняет установление фактических виновников.

5. Торговля краденым: использование дропов для продажи краденого

[1] Русскоязычный информационный сайт о криптовалюте Bitcoin [Электронный ресурс]. – URL: https://bits.media/silk-road/ (дата обращения: 20.02.2025).

имущества, чтобы скрыть идентичность настоящих преступников.

6. Шантаж: использование дропов для получения денежных средств от лиц, причастных к противоправной деятельности.

В любом из перечисленных выше преступлений «дроп» является промежуточным звеном в криминальной схеме. Если его используют с целью обналичить деньги с пластиковой карты, то «дроп», получив денежные средства на карту, через любой банкомат осуществляет снятие денежных средств и последующую передачу их иным лицам, участвующим в схеме, за получение процентов как вознаграждения от суммы снятия. При этом, пластиковые карты могут быть как зарегистрированы на дропа, так и краденными или полученными из-за границы криминальным путем. Что касается «дропа», который осуществляет оформление кредита на свое имя, то в данном случае он также получает процент от займа, а оставшуюся сумму передает иным лицам, и после этого кредит, естественно, не возвращается, а «дроп» исчезает. В случае организации контрабанды подконтрольных психоактивных веществ «дроп» осуществляет заказ и оплату через интернет-ресурсы предметов контрабанды, а также получение товара на свое имя в почтовых отделениях связи и передачу их лицам, организовавшим данный вид преступления, при этом получая вознаграждение. Это не исчерпывающий список преступных схем, где используются «дропы» и на сегодня существуют две самые распространенные и наиболее опасные для граждан Российской Федерации. К последним стоит отнести использования дропа при осуществлении телефонных мошенничеств, а именно, дроп может забрать лично денежные средства у жертвы, либо предоставить данные своей банковской карты для перевода на нее и дальнейшего обналичивания денежных средств.

Примечательно, что на сегодняшней день дропов из числа граждан Российской Федерации используют в своих преступных целях граждане других государств. Примером здесь может являться обнаруженное сотрудниками ФСВНГ Росгвардии в 2022 году в городе Бердянске здание, где раньше располагался «Кол-центр», целью которого являлось дистанционное хищение денежных средств со счетов граждан России. Количество рабочих мест насчитывало 70, где посменно

работало 300 человек, имеющих sip-телефоны с гарнитурой, при помощи которых в среднем совершалось около 5000 звонков в сутки. В данном кол-центре была организована четкая иерархия и IT-инфраструктура, а именно, осуществлялась закупка баз данных будущих жертв, обучение персонала, разбивка мошенников на группы, из которых одни совершали звонки, а другие прорабатывали схемы получения и вывода денежных средств через дропов. Обналиченные дропами денежные средства переводились через криптокошельки. Помимо вышеуказанных лиц в «кол-центре» также работали и технические специалисты, которые как настраивали оборудование, так и разрабатывали программное обеспечение для фиксации информации об операциях, счетах, вкладах и возможностях работы с жертвами. Примечательно, что параллельно с развитием «Кол-центров» в Украине, которых, к слову, насчитывается около 3000, начало совершенствоваться и качество предоставления услуг дропов. В даркнете довольно успешно, а главное долго функционируют ряд сервисов таких, как Darkmoney или Dublikat, где без проблем можно купить как реквизиты дебетовых карт, так и найти дропов для выполнения различных задач. В свой черед, онлайн-сервисы, которые подбирают дропов, за повышенный процент гарантируют заказчику возврат денег. Так, например, при подборе дропов онлайн-сервис требует от последнего внесение депозита в размере от 50000 тысяч рублей[1].

Используя в качестве источника ресурсы сети Интернет, злоумышленник может получать, использовать и даже рассекречивать как конфиденциальную информацию, так и информацию, представляющую государственную тайну. Впоследствии такие действия создают угрозу не только конкретному человеку, но и государству в целом. В качестве примера можно привести деятельность сайта «WikiLeaks» – международной некоммерческой организации, которая публиковала секретную информацию, взятую из анонимных источников или полученную при ее утечке[2].

---

[1] Анализ системы вывода денежных средств, похищенных у граждан [Электронный ресурс]. Сайт sberbank.ru URL: https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv?tab=analiz_problemy (дата обращения: 18.02.2025).

[2] About What is Wikileaks? [Электронный ресурс]. URL: https://www.wikileaks.org/About.html (дата обращения: 26.01.2025).

Л.Н. Игнатенко утверждает, что ввиду отсутствия достаточного числа специалистов в сфере информатики в правоохранительных органах получение полезной для расследования информации из компьютерной сети на практике достаточно проблематично. Решение данной задачи становится практически невозможным, если преступники, обладая профессиональными навыками работы с компьютером, уничтожают следы своей деятельности в компьютерной сети. Тогда расследованию может пригодиться информация о деятельности подозреваемого до и после совершения преступления, его встречах, покупках, денежных переводах и т. д.[1].

Такого же мнения и Л.П. Зверянская, которая пишет, что проблема выявления и предупреждения компьютерных преступлений – это высокая квалификация современных киберпреступников, не оставляющих следов присутствия и своего пребывания на месте совершенного преступления[2].

В целях решения вышеуказанных учеными проблем стоит начать с той истины, что любое преступление влечет за собой некое изменение в среде, то есть отпечаток или след, и данное суждение неоднократно на практике подтверждалось криминалистикой.

В связи с этим необходимо рассмотреть правовые и практические механизмы, направленные на исследование источников информации, в том числе записанные в них следы, которые прямо или косвенно указывают на противоправную деятельность, совершаемую при помощи компьютерных технологий.

Для достижения поставленной цели стоит обозначить, что, пользуясь благами компьютерных систем, пользователи зачастую даже не подозревают о том, что оставляют в ней следы своей деятельности, которые фиксируются в базах данных посещаемых ими ресурсов, а также на различном маршрутизирующем оборудовании. Возможность использования таких следов может быть рассмотрена в двух аспектах. С одной стороны, владельцы различных сервисов могут скрытно

---

[1] Игнатенко Л.Н. Организационно-тактические особенности проведения обыска по компьютерным преступлениям // Российский государственный педагогический университет им. А.И. Герцена. – 2016. – № 10(12). – С. 51.

[2] Зверянская Л.П. Дискуссионные проблемы выявления и предупреждения киберпреступлений // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 8. – С. 161.

отслеживать и анализировать действия пользователей с целью улучшить работоспособность своих сервисов, а с другой стороны – реализуют возможность ограничения доступа к информационным ресурсам, как отдельным пользователям, так и целым государствам.

Пользователь же и сам легко может ограничить доступ к своему компьютеру при помощи парольной защиты или специально созданного для таких целей программного обеспечения. Из чего вытекает, что, в техническом плане, источники могут быть как открытые (для общего пользования), так и с ограниченным доступом. Перспективными источниками стоит считать и базы данных различных учреждений, организаций и предприятий, где хранится информация о деятельности работающих там лиц, а также может фиксироваться их действия в сети Интернет.

Умелое использование и доступ к таким источникам компьютерной информации поможет сотрудникам ОВД зафиксировать и в дальнейшем анализировать преступную деятельность пользователей компьютерной сети. Безусловно, движение компьютерной информации должно контролироваться и вызывать интерес у сотрудников правоохранительных органов. Ведь, если получить доступ и проанализировать содержание компьютерной информации, которая вызывает интерес у пользователей, то можно спрогнозировать их действия в реальном мире. А.Г. Волеводз считает, что ставшая известной информация о прохождении сведений по электромагнитным системам связи, таким, как «сведения о сообщениях, передаваемых по сетям электрической связи» стоит называть компьютерными следами. Это могут быть также «исторические данные» об уже проведенных сеансах связи, или «данные о потоках информации», хранящихся у провайдеров[1].

Помимо компьютерных следов В.В. Борисов вводит понятие «информационных следов», которые обозначают некоторую информационную запись, сделанную на компьютерной технике подозреваемыми в преступлении лицами с помощью специального программного средства[2]. Однако сам след и есть

[1] Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. – 2002. – № 1. – С. 5.

[2] Борисов В.В. Об особенностях фиксации информационных следов в практике защиты информации //

информация, поэтому данную терминологию можно считать несовместимой с компьютером. Рассматривая следы преступлений, ученые, криминалисты разделяют их на виртуальные, материальные и идеальные[1].

Исследование, проведенное О.Ю. Введенской, в котором она значительное внимание уделяла анализу современной преступности, показало, что интернет-деятельность оставляет за собой материальные следы, – так считают 24 % опрошенных сотрудников ОВД, идеальные следы в виде показаний потерпевших, свидетелей, подозреваемых, обвиняемых – 22 %, виртуальные следы в виде кэш-файлов, IP-адресов, журналов историй, Log-файлов и т. п. – 27 %. Также 27 % опрошенных отмечают, что одним из важнейших элементов следовой картины рассматриваемой категории преступлений является информация, оставленная преступниками в сети Интернет, например, контакт с жертвой (переписка, фотографии, всевозможные записи и т. п.)[2].

В.А. Мещеряков также предлагает назвать компьютерные следы виртуальными. В понимании В.А. Мещерякова, виртуальные следы – это любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации[3].

Точки зрения, что виртуальные следы могут дополнить существующую в криминалистике классификацию следов, придерживается и А.В. Манукян[4].

Л.В. Борисовой предлагается определять виртуальные следы как информационные, остающиеся на машинных носителях, зафиксированные в программах, базах данных и текстовых файлах в течение времени совершения преступления как при непосредственном, так и удаленном доступе[5].

Известия ЮФУ. Технические науки. – 2009. – № 5. – С. 164.

[1] Баринов С.В. Следы преступных нарушений неприкосновенности частной жизни как элемент криминалистической характеристики / Вестник Удмуртского университета. серия экономика и право Издательство: Удмуртский государственный университет (Ижевск). – 2016. – № 1(26). – С. 86.; Криминалистика: учебник / под. ред. Е.П. Ищенко. – М.: Проспект, 2011. – С. 156.

[2] Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 211.

[3] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук: 12.00.09 / Владимир Алексеевич Мещеряков. – В., 2001. – С. 33.

[4] Манукян А.В. Виртуальные следы реальных преступлений // Мир юридической науки. – Санкт-Петербург. – 2015. – № 3. – С. 69.

[5] Борисова Л.В. Транснациональные компьютерные преступления как объект криминалистического исследования: автореф. дис. … канд. юрид. наук: 12.00.09 / Борисова Лариса Владимировна – К., 2007. – С.17.

Ученые В.А. Давыдов и А.Ю. Головин также дают своё определение виртуальным следам, которые представляют собой зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентских электронных устройств (терминалов, биллинговых систем и т. п.), вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления. В то же время ученые, рассматривая механизм подобного следообразования, указывают на следующие стадии: физическое проявление свойств следообразующих объектов (изображение, температура, отсчеты времени, звук и др.); преобразование исходной физической формы проявления следообразующего объекта в цифровую форму; предварительная обработка, передача и хранение полученной цифровой информации[1]. Из рассмотренного учеными механизма возникает вопрос, почему бы следы не назвать цифровыми, ведь такой термин встречается часто в употреблении среди ученых[2]. Изучения способа совершения преступления, где преступником были применены компьютерные технологии и в соответствии с их использованием достигнут преступный результат, укажут на соответствующие компьютерные следы преступления[3]. Так, В.Б. Вехов предлагает ввести в криминалистический категориальный аппарат новое понятие «электронно-цифровой след», под которым предлагает понимать «любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов». Мнение В.Б. Вехова не совпадает с мнением В.А. Мещерякова, А.В. Манукяна, Л.В. Борисовой по причине, как он считает, ошибочности термина «виртуальный», обосновывая это тем, что этот термин происходит от латинского virtualis, который означает «не имеющий

[1] Давыдов В.О., Головин А.Ю., Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия тульского государственного университета. экономические и юридические науки. – Тула., 2016. – № 3-2. – С. 255.

[2] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. ... канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. – М, 2018. – С.106.

[3] Комаров И.М. «Цифровая криминалистика» – давно назревшая проблема // Библиотека криминалиста. Научный журнал. – 2018. – № 2(37). – С. 165.

физического воплощения или воспринимаемый иначе, чем реализован в действительности». При этом ученый акцентирует внимание на том, что с позиций криминалистики «виртуальных следов» не может быть в принципе[1].

А.О. Сукманов же подчеркивает, что, кроме специалистов-физиков, в основной массе большинство людей (в том числе ученых-криминалистов и практиков – работников правоохранительных органов) термин «виртуальный» применяют и понимают именно в отношении компьютерного, цифрового пространства. Именно в этом понимании используется термин «виртуальность» во многих сферах современной жизни[2]. На наш взгляд, все же стоит использовать правильную терминологию, и не потому, что некоторым отраслям наук и отдельным исследователям так удобно, а именно с целью повышения качества законодательного применения.

Следует согласиться с позицией В.А. Левченковой, которая акцентировала внимание на том, что, несмотря на достаточно высокий уровень познания в сфере компьютерных технологий и закономерностях функционирования информационно-компьютерного пространства, виртуальные следы до сих пор не нашли своего места в криминалистической технике. Предполагаем, что В.А. Левченкова не поддерживает позицию В.А. Мещерякова относительно того, что виртуальные следы условно занимают промежуточное положение между следами материальными и идеальными, связывая это с тем, что материальные следы образуются в результате механического контакта материальных следообразующего и следовоспринимающего объектов. Идеальные следы, в свою очередь, хранятся в сознании людей, и никакого материального отображения не находят. Образование же виртуальных следов, хоть и отличается от образования следов материальных, но все же происходит на материальных носителях, и, соответственно, такие следы тоже имеют материальное выражение. Кроме того, в отличие от идеальных следов, материальные и виртуальные следы можно извлечь

---

[1] Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В.Б. Вехов. – Волгоград: ВА МВД России, 2008. – С. 95.

[2] Сукманов А.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений / Вестник Калининградского Филиала Санкт-Петербургского университета МВД России // – Калининград, 2010. – № 4. – С. 106.

и исследовать. Исходя из вышесказанного, наиболее верной представляется точка зрения о том, что рассматриваемые следы следует отнести к особой форме следов-отображений, зафиксированных на электронных носителях информации[1] при помощи компьютерной техники.

Как правильно указывает Н.В. Костякова, будучи следом, компьютерная информация, как и любой след, отображает факт взаимодействия материальных объектов. Однако при этом такая информация имеет отличительное качество: компьютерная информация легко может быть изменена либо уничтожена, причем, перечисленные действия могут производиться удаленно[2].

При расследовании компьютерных преступлений, отмечает А.Ю. Семенов, всегда важно учитывать, что следы, указывающие на факт работы подозреваемого на конкретном компьютере, не имеют практически никакой ценности. Причиной этому служит, как полагает исследователь, тот факт, что нередко орудием рассматриваемых преступлений и в то же время источником компьютерной информации является домашний или служебный компьютер подозреваемого, который используется им постоянно[3]. Однако, высказывая подобные суждения, важно было также обращать внимание на то, что источник в сфере компьютерной информации имеет ряд существенных отличительных признаков, который никоим образом не может быть сведен только лишь к домашнему или служебному компьютеру подозреваемого. Поэтому представление о следообразовании преступной деятельности в сфере компьютерных технологий и дальнейшей криминалистической фиксации следов такой деятельности требует рассмотрения обозначенной проблемы под несколько иным углом зрения.

Полагаем, что при раскрытии и расследовании компьютерных преступлений нужно исследовать те следы, которые образуются как в компьютере пользователя,

---

[1] Левченкова В.А. Современные научные подходы к формированию учения о виртуальных следах // Сборник материалов III Международной студенческой научно-практической конференции «Уголовно-процессуальный кодекс Российской Федерации: достижения и проблемы применения». – Курск., 2016. – С. 107.

[2] Костякова Н.В. Проблемы отыскания и изъятия виртуальных следов преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети интернет и мобильной связи // Вестник Барнаульского юридического института МВД России. – 2016. – № 2(31). – С. 125.

[3] Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. – 2004. – № 1. – С. 53.

так и путем преобразования в результате прохождения информации по самим техническим каналам связи. Стоит понимать, как устроен механизм передачи информации. Для взаимодействия устройств в компьютерных сетях разработана семиуровневая модель OSI (Open Systems Interconnection), где понятно, что информация на первоначальном уровне передается в виде электрических сигналов, световой волны или радиоволны. На следующих уровнях, а именно, после того, когда информация доходит до компьютерного устройства, происходит ее преобразование в цифровую, далее информация разбивается на блоки, называемые «пакетами». Также происходит стандартизация протоколов и интерфейсов с последующим преобразованием данных в понятный для пользователя вид, а именно, в компьютерную информацию. Для получения и передачи компьютерной информации устройства пользователей подключаются к операторам связи, у которых для таких целей имеются маршрутизирующие серверы с установленным на них специальным программным обеспечением. Стоит указать, что передаваемая при помощи операторов связи информация, должна быть защищена путем шифрования.

Так, в процессе передачи компьютерной информации, интерес представляет именно «пакет», который состоит из заголовка, включающего адреса отправителя и получателя, и полезной нагрузки или сообщения, которые передает сам пользователь.

При расследовании преступлений больший интерес, как правило, 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 о связях преступника, времени и месте совершения преступления. Если рассматривать следы, образуемые в технических каналах связи, то обычно они представляют собой сведения о сообщениях, передаваемых по данным сетям, которые могут сохраняться в техническом оборудовании провайдеров связи и аккумулироваться в специальных текстовых файлах, куда компьютерная система записывает информацию о работе устройства или сервиса, так называемых Log-файлах. Например, в этих Log-файлах

могут находиться данные о том, кто инициировал данное сообщение, когда и в какое время оно произошло и какие файлы затронуло. По существу, в них протоколируется техническая информация, содержащая данные об информационно-технологических процессах обработки информации и представлении ее потребителю[1].

Чтобы ориентироваться и сопоставлять информацию, которая встречается в логах различных приложений, нужно иметь представление о том, что и как пишется в Log-файлах.

Для того, чтобы получить информацию из логов, достаточно текстового редактора, но для анализа и структурирования информации необходимо применить определенный интерфейс. В этом случае необходимо знать механизм логирования и особенности структуры Log-файлов, а также информации, которая в них встречается. В свою очередь, Log-файлы подразделяются на:

1. Текстовые Log-файлы, которые делятся на:

- способ, при котором событие представляет собой отдельную строку;

- логи, в которых отдельное событие представляет собой не одну строку, а несколько.

Такой Log-файл гораздо сложнее для анализа, так как каждое событие может представлять собой набор мелких записей. Для чтения таких логов чаще всего используется специальное программное обеспечение.

2. Бинарный Log, который представляет собой тип логов, для чтения которых нужна специальная программа, с помощью которой бинарный Log и анализируется[2].

Система записывает Log-файлы незаметно для пользователя, используя алгоритмы, предусмотренные производителем программного обеспечения.

Иногда логирование необходимо установить и включить, отредактировав конфигурационный файл, в котором может настраиваться имя файла, директория

---

[1] Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10. – С. 92.

[2] Логирование информации [Электронный ресурс]. – URL: http://hostinfo.ru/articles/security/rubric157/1062/ (дата обращения: 15.01.2025).

или полный путь к тому файлу, в который пишется Log-файл.

Это очень полезно, если процесс логирования необходимо записывать на отдельный жесткий диск или сетевой диск и т. д. Такой способ удобен, если логи будут интерпретироваться сторонним приложением, которое находится на отдельном компьютере.

В зависимости от настройки система каждый день, неделю, месяц и т. д. использует новый Log-файл. Обычно, если изменение Log-файлов связано с вычислением времени (каждый день, каждый год и т. п.), то в имени используется время (дата и время или только дата, иногда какая-то производная) создания или финального закрытия данного Log-файла.

Набор событий, которые логируются, всегда можно настраивать. Это решает часть проблем с производительностью.

Чаще всего операционная система предоставляет свои профили логирования от полного исключения и до полного логирования всего происходящего. Есть возможность указать даже не профиль, а настройки логирования для каждого конкретного события. Такие настройки позволяют сделать гибкое логирование информации, необходимой в конкретном случае.

На наш взгляд, к операторам связи и интернет-провайдерам необходимо относиться как к источникам информации, которая может иметь значение при расследовании преступлений. Желательно, чтобы такая информация сохранялась в текстовом файле и по запросу от правоохранительных органов передавалась на выделенный удаленный сервер хранения Log-файлов МВД. Содержание указанной информации могут составлять данные о:

1) IP-адресе компьютера, под которыми пользователь заходил в Интернет;

2) IP-адресе и полных ссылках посещаемого ресурса;

3) дате и времени осуществления перехода на ресурс;

4) размере полученного и переданного трафика.

Существенным добавлением к этой информации, а именно к п. 1, будут и те данные, которые провайдер получает при заключении договора с каждым пользователем своих услуг – такие, как: паспортные данные пользователя, место

проживания, номер телефона и т.д.

При расследовании компьютерных преступлений кроме Log-файлов важно обращать внимание на программное обеспечение и содержание файлов, где содержатся тексты документов, фотоизображения, видео- и аудио-фрагменты и т. п., которые также представляют собой следы преступлений.

Так, например, компьютерная информация, имеющая значение в расследовании преступления, может храниться и на компьютерном устройстве, при помощи которого осуществлялись передача и получение информации. Операционная система, например, Windows, регистрирует и сохраняет все происходящие на компьютере события (ошибки, время запуска приложений, время входа на компьютер и т. п.), которые можно увидеть в журнале событий. В браузере пользователя, а именно в разделе «история», можно получить сведения о посещении и времени перехода на сайт. В разделе «загрузки» отображается история скачанных файлов. Также в браузере хранятся закладки, логины и пароли сайтов, где регистрировался пользователь и т. д. Интерес могут представлять графические и текстовые редакторы, в свойствах которых отображается кто, когда и в какое время создал файл.

В большинстве случаев источником данных может выступать разработчик программного обеспечения, который шифрует передаваемую информацию. В открытом доступе такую информацию получить очень сложно. В первую очередь, это связанно с использованием различных алгоритмов шифрования данных, передаваемых при помощи компьютерной сети.

Поэтому, чтобы оперативно искать и получать компьютерную информацию при помощи данных, передаваемых посредством шифрования в компьютерной сети, необходимо понимать механизм циркуляции компьютерной информации, а именно, как происходит передача компьютерной информации и что необходимо задействовать для получения и использования ее в оперативных нуждах.

Помимо оборудования пользователей и операторов связи, компьютерная информация также находится на различных серверах и сохраняется при помощи специального программном обеспечении, установленного на последних. К таким

стоит отнести Веб-сервера, файловые сервера, облачные сервера, игровые сервера, почтовые сервера, прокси-сервера, VPN-сервер, DNS-сервера и другие. Рассмотрим некоторые из них как источники компьютерной информации, представляющей интерес для расследования преступлений.

Веб-сервер предназначен для хранения и обработки данных веб-сайтов. На Веб-сервер устанавливается серверное программное обеспечение, позволяющее работать веб-сайтам и приложениям. К ним можно отнести поисковые системы (отечественные «Яндекс», «Mail.ru», Google, Yahoo), социальные сети («ВКонтакте», «Одноклассники»), мессенджеры – («Telegram», «Viber», «WhatsApp», «Skype», «WeChat»), сайты объявлений (Avito, youla) и другие сайты. Файловый сервер, как и облачные, нужен для хранения и упорядочивания больших объёмов файлов и предоставления к ним доступа пользователей сети. VPN- и прокси-сервера выступают промежуточным звеном между пользователем и онлайн ресурсом. VPN- в отличии от прокси-сервера использует зашифрованный канал связи. Чтобы сайт попал в поисковую систему и в последствии появился в выдаче на запрос, разработчик должен его туда добавить. Также есть сайты, которые не индексируются поисковыми системами и для доступа, к которым используются нестандартные программы (Tor-браузер), порты и протоколы.

Необходимо подчеркнуть, что все те данные, которые пользователь запросил при помощи поисковых сервисов и оставил, например, в социальный сети с момента регистрации, хранятся длительный промежуток времени в базе данных таких сайтов и даже после удаления его профиля.

В социальных сетях пользователи в процессе регистрации указывают огромное количество информации, которое также является источником, имеющим значение при раскрытии и расследовании преступлений. Так, например, чтобы стать пользователем социальной сети «ВКонтакте», нужно пройти регистрацию. При регистрации необходимо заполнить регистрационную форму, состоящую из полей, в которых пользователь указывает такие анкетные данные, как ФИО, страну и город проживания, контактный телефон, электронный почтовый адрес. После регистрации все сведения, которые пользователь внес в регистрационную форму,

записываются и хранятся в базе данных сайта для дальнейшей авторизации пользователя. С вышеуказанной информацией в базе данных сервера, где размещена социальная сеть, записываются и хранятся:

- дата регистрации пользователя на сайте;

- IP-адрес компьютера, с которого производилась регистрация;

- данные о версии браузера и операционной системы, при помощи которой осуществлялась регистрация.

Полученная информация владельцем сайта очень часто используется, например, как статистические данные. Эти данные фиксируются и далее по принципу работы логирования могут визуально отображаться специальным программным обеспечением. Процесс фиксации статистических данных происходит скрытно и зачастую без ведома пользователя. Такая информация может выступать не только как статистическая, но также иметь огромное значение при поиске и фиксации мест хранения и обмена данными лицами, которые осуществляют противоправные действия в сети Интернет.

Можно заключить, что одной из основных целей ресурсов в сети Интернет является не только предоставление интересующей компьютерной информации пользователю, но также накапливание данных о его действиях[1], что возможно и нужно использовать как источник компьютерной информации для решения задач в расследовании преступлений. Политика конфиденциальности поисковой системы Google является тому подтверждением, ведь все запросы в данной поисковой системе и переходы по страницам сайтов записываются, хранятся и продуктивно используются в различных целях самой системой, в том числе и для борьбы с преступностью[2].

Здесь стоит отметить, что количество источников компьютерной информации постоянно возрастает, однако, законодательные механизмы, призванные урегулировать такую деятельность, не изменяются, что играет на пользу

[1] Павлюков В.В. Правовые аспекты получения и защиты компьютерной информации в сети Интернет // Вестник Дальневосточного юридического института МВД России. – 2017. – № 3(40). – С. 180.

[2] С 1 марта Google официально следит за каждым. [Электронный ресурс]. – URL: http://techno.bigmir.net/technology/1516551-S-1-marta-Google-oficial-no-sledit-za-kazhdym- (дата обращения: 20.02.2025).

злоумышленникам. В связи с этим злоумышленник при регистрации на ресурсах сети Интернет, указав ложные данные, считает, что невозможно установить информацию о его местонахождении и получить реальные анкетные данные последнего.

Однако, рассматривая сферу информационных технологий как источник компьютерной информации, используемой в расследовании преступлений, мы приходим к выводу, что данные о времени подключения к компьютерной сети, о посещаемых ресурсах, о передаваемом трафике интерпретируются без ведома пользователя, скрытно сохраняя следы его деятельности не только на тех ресурсах, которые он посещал, но и на той компьютерной технике, которая использовалась для обращения к этим ресурсам.

В связи с этим можно предположить, что для того, чтобы получить первоначальные данные о совершаемом и совершенном преступлении при помощи компьютерной информации, необходимо получить статистические (адресные) данные, которые при помощи функций операционной системы сохраняются и хранятся в Log-файлах. Источником такой информации является как оператор связи, интернет- и хостинг-провайдер, т. е. организация, которая предоставляет услуги связи и пространство для хранения данных, так и компьютеры и периферийные устройства пользователей. Впоследствии возможно установить и содержательную часть передаваемых при помощи компьютерных систем сообщений, которые также должны храниться в базах данных владельцев интернет-ресурсов или разработчиков программного обеспечения.

Безусловно, такая информация содержит в себе ограничения доступа, прописанные статьей 9 Федерального закона «Об информации, информатизации и защите информации». Из закона также известно, что правовой защите подлежит любая документированная информация, т. е. информация, облеченная в форму, позволяющую ее идентифицировать[1].

Подводя итоги параграфа, предложим свою классификацию источников

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.01.2025).

компьютерной информации, которые должны учитываться в процессе расследования преступлений:

По способу передачи: электрические провода 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-сервера, сервера 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:

- не зашифрованные 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 комбинациий 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 таким относятся как ресурсы сети Интернет с ограниченным доступом, так и компьютерные устройства (стационарные компьютеры, ноутбуки, мобильные телефоны, планшеты, аудио и видео регистраторы, сервера, 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. Подчеркнем, что практически любую компьютерную информацию из открытой можно сделать с ограниченным доступом.

Такая классификация позволяет более точно определить, откуда можно получить компьютерную информацию правоохранительными органами, а также учесть факторы безопасности и доступа к данным.

Вместе с тем, для получения компьютерной информации как из открытых источников, так и источников с ограниченным доступом, необходимо иметь достаточно навыков и законных оснований. Возникает необходимость рассмотреть более детально шаги, сделанные законодателем, с целью получения и использования компьютерной информации правоохранительными органами из рассматриваемых нами источников.

Именно поэтому необходимо проанализировать возможные правовые нормы доступа и получения компьютерной информации ОВД как в российском, так и в зарубежном законодательстве, сконцентрировав свое внимание на доступе к компьютерной информации, при помощи которой возможно своевременно оказать противодействие преступности.

§ 1.3. Правовая регламентация доступа правоохранительных органов к компьютерной информации, используемой в расследовании преступлений: российский и зарубежный опыт

В настоящее время вопрос правового регулирования движения компьютерной информации активно обсуждается большинством государств. Обращаясь к международной законодательной практике регулирования информационных процессов, необходимо прежде всего отметить, что основной сферой регулирования на сегодняшний момент является сфера регулирования оборота данных в сети Интернет, что подтверждается анализом многочисленных нормативно-правовых актов различных государств[1].

Это связанно с тем, что определенные субъекты, получающие информацию из компьютерной сети, в дальнейшем используют ее в преступных целях. Кроме того, сама компьютерная информация уже изначально может иметь противоправный характер или указывать на преступную деятельность физического или юридического лица.

Депутат Госдумы РФ И.А. Яровая акцентировала внимание на том, что в мировой практике механизмы регулирования движения компьютерной информации в телекоммуникационных сетях в контексте деятельности правоохранительных органов являются давно опробованными и востребованными[2]. Добавим, что уникальная возможность компьютерных данных представляется также и в том ключе, что в случаях сохранения таких данных до момента совершения преступления, с помощью последних можно воссоздать картину совершенного преступления, а также проанализировать и выявить противоправные действия на стадии подготовки к следующему противоправному деянию.

---

[1] Кучина Я.О. Облачные технологии: понятие и основы правового регулирования // Дальневосточный федеральный университет, г. Владивосток. – 2016. – № 4. – С. 83.

[2] Яровая объяснила, для чего нужен новый пакет законов [Электронный ресурс]. – URL: http://www.vestifinance.ru/articles/72602 (дата обращения 25.01.2025).

Но чтобы процесс использования компьютерных данных в целях противодействия преступности стал эффективным, необходима продуманная модель управления действиями сотрудников правоохранительных органов, а также разработка законодательной базы, позволяющая правоохранительным органам как фиксировать, так и получать доступ к определенной компьютерной информации.

Отметим, что на международном уровне предпринимались попытки законодательного закрепления подобных механизмов противодействия киберпреступности. В законе «Об оперативно-розыскной деятельности (новая редакция)», принятом на 27-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (Постановление от 16.11.2006 № 27-6), было упомянуто мероприятие под названием – «Мониторинг информационно-телекоммуникационных сетей и систем». Данное мероприятие определили как «…получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам»[1].

Российская нормативная практика тоже подключилась к урегулированию процессов противодействия киберпреступности. Федеральным законом от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» статья 185 УПК РФ была дополнена ч. 7 следующего содержания: «При наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях,

[1] Модельный закон «Об оперативно-розыскной деятельности» (новая редакция) [Электронный ресурс] Электронный фонд правовых и нормативно-технических документов //. – URL: https://docs.cntd.ru/document/902050857 (дата обращения: 15.01.2025).

следователем по решению суда могут быть проведены их осмотр и выемка»[1].

Из анализа содержания указанной нормативной новеллы можно сделать вывод о том, что в последней сделан акцент на электронных и иных сообщениях, а именно, информации, переданной или полученной пользователем информационно-телекоммуникационной сети. Под действие ч. 7 ст. 185 УПК РФ подпадают все сообщения, которые абонент и (или) пользователь любого мобильного компьютерного устройства может отправить через сервис коротких сообщений сетей сотовой связи, программы-приложения для мобильных операционных систем, мессенджеры, а также с помощью технологий IP-телефонии[2].

Еще один аспект, на который следует обратить внимание в спектре обозначенных рассуждений – это то, что требует признания представителями международного сообщества, а также представителями власти внутри каждого государства, на целесообразности применения совместных усилий подразделений правоохранительных органов в деле расследования преступности, совершаемых в сфере компьютерной информации. Современные реалии свидетельствуют о том, что не существует проблем отдельно для каждого государственного органа или его отдельного подразделения, поскольку все проблемы правоохранительного характера решаются совместными усилиями путем взаимодействия[3]. Прямое указание на взаимодействие при совместном противодействии преступности мы находим в ФЗ № 3-ФЗ «О полиции», в ст. 10 «Взаимодействие и сотрудничество»[4].

Вышеуказанное побуждает представителей юридической науки изучать отечественный законодательный опыт регулирования процедур использования компьютерных технологий, в том числе и в сфере правоохранительной

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06 июля 2016 № 375-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

[2] Меньшова П.Э. К вопросу о нормативном регулировании и применении оперативно-розыскного мероприятия «Получение компьютерной информации» // Научно-методический электронный журнал «Концепт». – 2017. – № 39. – С. 879.

[3] Алиуллов Р.Р., Саетгараев В.Ф. Сущность и основные принципы взаимодействия подразделений полиции в сфере реализации оперативно-служебных задач // Вестник Казанского юридического института МВД России. – 2015. – № 2(20). – С. 71.

[4] О полиции: Федеральный закон от 07 февраля 2011 № 3-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

деятельности, а также анализировать и перенимать положительный зарубежный опыт законодательного закрепления права правоохранительных органов на получение доступа к компьютерной информации в целях раскрытия и расследования преступлений.

Исторический анализ законодательного регулирования рассматриваемого нами аспекта проблематики показывает, что отправной точкой зарождения законодательства, связанного с регулированием информационных правоотношений в компьютерной среде, можно считать принятый в 1978 году в Соединенных Штатах Америки (далее - США) в штате Аризона закон «Computer crime act of 1978». Подобная законодательная практика была воспринята и другими американскими штатами, в которых были приняты похожие законодательные акты.

Главной особенностью упомянутого нормативного акта американского законодательства является то, что он установил ответственность за «Несанкционированное использование вычислительных средств». Кроме того, в ст. 815.03 этого закона также впервые дано определение «Доступа» к компьютерной информации, который подразумевает подход, инструктирование, обмен, хранение информации, ее извлечение, а также использование ресурсов компьютера, компьютерных систем и сетей любым возможным образом[1].

Интерес представляет и статья 815.06 упомянутого нормативного документа, где указано, что в случаях преступлений против пользователей компьютеров к ответственности необходимо привлекать тех, кто намеренно, сознательно и без разрешения все же осуществляет доступ к любому компьютеру, компьютерной системе или компьютерной сети; отрицает или отказывает в предоставлении авторизованному пользователю таких компьютерных системных услуг, которые предоставляются по договору. Как видим, из содержания статьи становится понятным, что доступ к компьютерной информации должен осуществляться с разрешения пользователя компьютера.

В.Г. Степанов-Егиянц в свое время предложил разделять доступ к

[1] Computer crime act of 1978: Закон США [Электронный ресурс]. – URL: http://docweb.cns.ufl.edu/docs/d0010/d0010.html (дата обращения: 13.02.2025).

компьютерной информации на непосредственный, опосредованный, удаленный и смешанный[1]. Однако, если внимательно посмотреть на содержание упомянутой статьи, то можно заметить, что американский законодатель упустил в своем подходе вопрос целесообразности нормативного урегулировании ответственности за физическое подключение и доступ к компьютерной сети без разрешения ее владельца или удаленное подключение, под которым все чаще принято считать удаленное получение компьютерной информации.

Обоснованность восполнения указанного законодательного пробела не заставила себя долго ждать, правоприменительная практика стала указывать на целесообразность разрешения обозначенной проблемы. Известен в международной практике факт, что в 1969 г. Альфонсе Конфессоре, получив незаконно доступ к информации в электронно-вычислительной сети, совершил налоговое преступление, ущерб от которого составил $620 000[2]. Как можно заметить, осуществление преступного умысла было реализовано благодаря незаконному доступу к компьютерной информации, после чего злоумышленник путем манипуляций с компьютерными данными получил колоссальную выгоду.

Когда первоначально различные государства стали сталкиваться с совершением преступлений при помощи компьютерной техники, то их правоохранительные органы (а затем и Россия) начали вести борьбу с такой преступностью путем применения к виновным традиционных норм о хищениях или злоупотреблениях. Но спустя некоторое время пришло осознание того, что такой подход является неэффективным, поскольку, во-первых, компьютерные преступления не укладываются в диспозиции норм об ответственности за названные преступления. Во-вторых, также был не учтен способ совершения компьютерных преступлений[3].

На данном историческом этапе развития законодательства в сфере

---

[1] Степанов-Егиянц В.Г. К вопросу о месте совершения компьютерных преступлений // Армия и общество. – 2014. – № 5(42). – С. 19.

[2] Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник Удмуртского университета. Серия Экономика и право. – 2011. – № 4. – С.114-115.

[3] Беспалова Е.В. Киберпреступность: история уголовно–правового противодействия // Информационное право. – 2006. – № 4(7). – С. 3.

противодействия киберпреступности, нормативное регулирование в области информационных технологий не ставило перед собой целью контролировать движение компьютерной информации и пресекать его на стадии совершения преступления (тем более на стадии подготовки к совершению преступления), а лишь вводило наказания после факта совершения противоправного использования компьютерной техники. Поэтому не уделялось должного внимания фиксации действий в процессе совершения компьютерного преступления при помощи средств компьютерной техники.

В настоящее время, несмотря на сложность и новизну рассматриваемой проблематики, не только развивающиеся, но и развитые страны поддерживают инициативу международно-правового регулирования глобальной информационной сферы. Существует разница в подходах к определению угроз информационной безопасности в России и других государствах. Сущностное противоречие в подходах проявляется главным образом на уровне терминологии: если Россия инициирует обсуждение проблемы «информационной безопасности», включающей в себя как технические, так и социально-психологические аспекты, то США и ряд стран Европы полагают, что на международном уровне обсуждению подлежит лишь «кибербезопасность», то есть информационно-техническая проблематика[1].

Когда только начало развиваться законодательство США в сфере противодействия киберпреступности, то оно, как и предполагалось, действовало только лишь на территории американского государства, однако примечательной особенностью, как указывает А.В. Суслопаров, компьютерных преступлений является также их транснациональный характер[2]. Поэтому возникла необходимость урегулирования вопросов контроля Глобальной компьютерной сети и осуществления международного взаимодействия на законодательном уровне.

В этом плане Европейская Конвенция по киберпреступлениям, которая 23

[1] Зиновьева Е.С. Развитие информационного общества: проблемы безопасности // Вестник МГИМО. – 2012. – № 1. – С. 134.

[2] Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук: 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2010. – С. 5.

ноября 2001 года рассматривалась в Будапеште, стала отправной точкой в области регулирования ответственности за преступления, совершаемые в компьютерных сетях. Так, помимо разработки единых правовых стандартов борьбы с компьютерными преступлениями, в статьях 16, 17, 18, 19, 20, 21 данной Конвенции был отрегулирован вопрос получения компьютерной информации и ее дальнейшего использования в целях противодействия преступности. Указанный международный нормативно-правовой акт оговорил также вопросы принятия мер законодательного и иного характера, при которых будет обеспечено сохранение и предоставление компетентным органам компьютерных данных от поставщиков такой информации. Описан был в Конвенции и механизм оказания помощи компетентным органам в сборе или записи данных в режиме реального времени[1].

Примечательно, что упомянутый нормативный документ был доступен для подписания не только государствами-членами Совета Европы, но и не являющимися его членами странами, однако которые участвовали в его разработке. В итоге конвенцию подписали США, Канада, Япония, Южно-Африканская Республика и еще 38 стран-членов Совета Европы.

Представители российского государства отказались подписывать конвенцию, мотивируя свое решение тем, что изложенное в п. «b» ст. 32 положение рассматриваемого международного документа может причинить ущерб суверенитету и безопасности государств-участников Конвенции, а также правам их граждан[2]. Данный пункт содержал следующие предписания: «Сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему».

Некоторые исследователи по этому поводу заявили о том, что Россия ничего

[1] Конвенция о киберпреступности (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года [Электронный ресурс]. – URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения: 01.02.2025).

[2] Путин отказался подписать Конвенцию о киберпреступниках [Электронный ресурс]. – URL: http://safe.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu (дата обращения: 03.02.2025).

не теряла в результате того, если бы она решилась подписать Конвенцию. Однако Российское государство лишилось возможности обмениваться с другими странами компьютерной информацией, которая способствовала бы выявлению и раскрытию преступлений.

Прав, на наш взгляд, О.С. Алавердов, отмечая, что сейчас ни одно государство не в состоянии противодействовать преступлению, совершаемому при помощи компьютерной сети самостоятельно, используя лишь собственный государственно-властный механизм. Только благодаря постоянному тесному сотрудничеству мировое сообщество может противостоять такому фактору транснациональных угроз как интернет-преступность[1].

Обратим внимание на следующий аспект рассматриваемого вопроса. На пути к сохранению компьютерных данных в целях их дальнейшего использования определенными субъектами стояла со своими ограничениями Директива 95/46/ЕС Европейского Парламента и Совета Европы от 24 октября 1995 г. В этой Директиве обращалось внимание на то, что для обеспечения защиты обработки персональных данных, принадлежащих физическим лицам, а также для создания условий беспрепятственного перемещении таких данных, государства-члены должны были разработать действенные механизмы защиты прав и свобод человека в компьютерной сфере, обеспечив при этом свободный поток личных данных[2].

Позже Директива 2002/58/ЕС от 12 июля 2002 года, регулирующая вопросы обработки персональных данных и защиты конфиденциальности в секторе электронных коммуникаций, установила требования к сетям и услугам, используемым для обработки данных о трафике и местонахождении устройства, а также использования электронных услуг связи. В частности, соответствующие данные должны удаляться в тех случаях, когда необходимо отправить электронное сообщение, при этом сохраняются данные, необходимые для осуществления платежей за подключение услуг.

---

[1] Алавердов О.С. Международное сотрудничество в области борьбы с Интернет-преступностью // Общество и право. – 2010. – № 3(30). – С. 165.

[2] Directive 95/46/EC of the european parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Электронный ресурс]. – URL: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (дата обращения: 16.02.2025).

Следует также указать на то, что в соответствии с п. 1 ст. 15 Директивы 2002/58/ЕС государства-члены своим решением могут ограничивать объем прав и обязанностей. Однако такие действия должны быть взвешенными и пропорциональными в рамках демократического общества и реализовываться только в целях обеспечения общественного порядка, национальной и общественной безопасности, противодействия преступности, а также в случае выявления несанкционированного использования электронных коммуникационных систем. При этом информация, которую получают с помощью электронных сообщений, имеет существенное значение для предупреждения и раскрытия преступлений, она также предоставляет дополнительные возможности в противодействии преступности, на что обращалось внимание в выводах Совета юстиции и внутренних дел Совета Европы от 19 декабря 2002 г.

Помимо указанных доводов и сами сотрудники специальных правоохранительных служб неоднократно приходили к выводам о целесообразности сохранения данных, полученных с помощью средств связи, в целях дальнейшего их использования в деле расследования киберпреступности. Целесообразность сохранения данных в течение определенного периода времени в правоохранительных органах отображена также в Декларации о борьбе с терроризмом, принятой Советом Европы 25 марта 2004 г.

По нашему мнению, сохранение соответствующих данных является вполне прагматичным шагом и имеет особо важное значение для борьбы с терроризмом, организованной преступностью и другими преступлениями, а также способствует выявлению потенциальных террористов и преступных группировок. Показательным в этом плане является пример, когда удалось установить личности исполнителей теракта, причастных к взрывам 7 июля 2005 году в Лондоне. Это было сделано благодаря, в том числе, анализу компьютерной информации, запечатленной видеокамерами наружного наблюдения в системе видеонаблюдения[1]. Позже, 13 июля 2005 г. на внеочередном заседании Совета

[1] Теракты в лондонском метро 7 июля 2005 года. Справка [Электронный ресурс] РИА Новости. – URL: https://ria.ru/defense_safety/20090707/176530177.html (дата обращения: 24.02.2025).

Европейского Союза, осуждающем террористические акты в Лондоне, было указано на необходимость срочного принятия совместных мер по сохранению данных электросвязи, а также об обмене данными между правоохранительными органами[1].

Полагаем, что назрела необходимость обеспечения на европейском уровне сохранения в течение определенного периода данных, которые создаются и обрабатываются поставщиками услуг общедоступных электронных сообщений или общественных сетей связи. Однако необходимо при этом учитывать тот факт, что на упомянутом заседании было выдвинуто требование к указанным субъектам сохранять только те данные, которые создаются и обрабатываются в процессе предоставления своих услуг. Поэтому в том случае, когда такие данные не генерируются или обрабатываются теми поставщиками, они не обязаны хранить их. Стоит также добавить, что Директива не урегулировала вопрос согласования технологии для хранения данных, поскольку его разрешение было отдано на откуп национальному законодательству.

Но вот следующий примечательный шаг Европейского Союза – 15 марта 2006 года он принимает Директиву по хранению данных «О сохранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования и поправок к Директиве 2002/58/ЕС»[2] (Впоследствии 8 апреля 2014 года Суд Европейского союза объявил Директиву 2006/24/ЕС недействительной за нарушение основных конституционных прав[3]). Этим документом от 28-и государств-членов требуется обеспечить, чтобы провайдеры связи сохраняли необходимые данные, указанные в Директиве, в течение периода от 6 месяцев до 2 лет.

---

[1] Press release extraordinary council meeting justice and home affairs Brussels, 13 July 2005 [Электронный ресурс]. – URL: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf (дата обращения: 13.02.2025).

[2] Directive 2006/24/EC of the European parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Электронный ресурс]. – URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (дата обращения: 15.01.2025).

[3] European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014 [Электронный ресурс]. – URL: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN (дата обращения: 22.02.2025).

Данные должны быть доступны «компетентным» национальным органам в конкретных случаях «для целей расследования, обнаружения и преследования серьезных преступлений, как это определено каждым государством-членом в его национальном законодательстве».

Следует указать, что эта Директива охватывает фиксацию телефонной связи, доступ в Интернет, электронную почту и VoIP. Государства-члены должны были перенести его в национальное законодательство в течение 18 месяцев – не позднее сентября 2007 года. Все 28 государств ЕС уведомили Европейскую комиссию о переносе Директивы в свой национальный закон спустя некоторое время. Из них некоторые страны лишь частично заменили законодательство.

В соответствии с этой Директивой не могут храниться данные, которые свидетельствуют о содержании сообщения, то есть сохраняться должны только метаданные. Кроме того, первым из этапов реализации Директивы стало законодательное внедрение каждым государством массового обязательства поставщиков услуг сети Интернет сохранять метаданные о пользователях, их деятельности в сети и делать это за достаточно длительный промежуток времени. Члены-государства постепенно стали принимать нормативные акты, предусматривающее сохранение данных от поставщиков услуг, с целью предупреждения, расследования, выявления и преследования уголовных преступлений. Однако спустя определенный промежуток времени ряд стран стали отменять действия подобных нормативных документов. Причиной тому стало появление конкуренции между положениями таких нормативных актов и законодательными источниками внутринационального законодательства, гарантирующего на конституционном уровне права и свободы граждан.

Вот один из примеров, как сначала в Федеративной Республике Германии (далее-Германия) Немецкий Бундестаг стал осуществлять Директиву, реализовав ее в законе о Телекоммуникациях (Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen 2006/24/EG), который вступил в силу 1 января 2008 года. По этому закону любые данные связи должны были сохраняться в течение 6 месяцев. Однако в последствии,

2 марта 2010 года Федеральный конституционный суд Германии признал данный закон неконституционным в части нарушения гарантии секретности корреспонденции. Судебным органом было также указано, что данные о телефонных переговорах и электронной почты, хранящиеся в Германии, должны быть удалены[1].

Показательно, что по пути Германии пошли и другие государства, которые сначала имплементировали в национальное законодательство положения Директивы 2002/58/ЕС, а потом спустя некоторое время или путем отмены соответствующих нормативных актов, или путем признания их неконституционными отказались сохранять в национальной практике подобные механизмы противодействия киберпреступности. Так, например, указанная участь постигла, среди прочих, такие государства:

1) Чешскую Республику, где реализация Директивы сначала стала частью закона № 259/2010 Coll., распространявшегося на электронные сообщения, с последующими изменениями. Согласно ст. 97 (3) этого закона, данные электросвязи должны были храниться от 6 до 12 месяцев;

2) Румынию, в которой определенное время действовал подобный Закон под номером 298/2008;

3) Королевство Швецию (далее – Швеция) – она реализовала отдельные положения Директивы в мае 2012 года, закрепив в своем законодательстве право 6 месяцев хранить указанные данные;

4) Словацкую Республику (далее-Словакия) – это государство сначала приняло Закон № 610/2003 Coll. в целях имплементации положений упомянутой Директивы. По этому закону данные о телекоммуникациях должны были храниться в течение 6 месяцев, если они были связаны с Интернетом, электронной почтой Интернета и интернет-телефонией (ст. 59a (6) a)), а в течение 12 месяцев – в случае других видов связи (ст. 59a (6) Б))[2].

---

[1] German court orders stored telecoms data deletion [Электронный ресурс] News BBC. – URL: http://nzsxo4y.mjrgg.mnxs45ll.cmle.ru/2/hi/europe/8545772.stm (дата обращения: 22.02.2025).

[2] Telecommunications data retention [Электронный ресурс]. – URL: https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Telecommunications_data_retention.html (дата обращения: 18.02.2025).

Хотелось бы обратить внимание на то, что, хотя указанная Директива и принятые на ее основе национальные нормативно-правовые акты были отменены, все же некоторые государства посчитали целесообразным законодательно сохранить механизм накопления, хранения и использования компьютерной информации в целях противодействия киберпреступности.

Так, например, в Соединенном Королевстве Великобритании и Северной Ирландии (далее-Великобритания) регулирование полномочий государственных органов, осуществляющих надзор, расследование и перехват сообщений, осуществляется еще с 2000-го года на основании закона Regulation of Investigatory Powers Act 2000 (далее – RIPA). В законе RIPA перечислены органы, которые имеют доступ к сохраненным данным в Великобритании, а именно:

- полицейские силы;

- национальная служба криминальной разведки;

- агентство по борьбе с организованной преступностью, ранее занимавшееся национальной преступностью;

- таможня;

- секретная служба разведки;

- штаб-квартира государственных органов связи.

RIPA также наделяет полномочиями министра внутренних дел изменять список органов, имеющих доступ к сохраненным данным. В список уполномоченных органов входят:

- агентство по стандартам качества пищевых продуктов;

- местные власти;

- национальный центр здоровья.

Обоснования для доступа к сохраненным данным в Великобритании, изложенные в RIPA, включают:

- интересы национальной безопасности;

- предотвращение или обнаружение преступлений или предотвращение беспорядков;

- экономическое благосостояние Великобритании;

- общественную безопасность;

- защиту общественного здоровья;

- оценку или взимание любого налога, пошлины, сбора или другого наложения, взносов или сборов, подлежащих уплате государственному департаменту;

- любую другую цель, не указанную выше, которая указана для целей настоящего подраздела в порядке, установленном государственным секретарем[1].

На основании Акта по борьбе с терроризмом, преступностью и безопасности (Anti-Terrorism, Crime and Security Act) спецслужбы Великобритании имеют право получать пользовательскую информацию у операторов без решения суда, а лишь на основании решений Министерства внутренних дел или других высокопоставленных чиновников. Интересный момент: в Великобритании перехват данных легализован не только для государства. В 2001 г. был принят закон, разрешающий компаниям прослушивать рабочие телефонные линии и просматривать корпоративные адреса электронной почты своих сотрудников[2].

Документы, полученные из Ассоциации главных полицейских, показали, что Великобритания также планирует собирать данные из общенациональной сети видеокамер распознавания номерных знаков и хранить данные в течение 2-х лет. Эти данные затем могут быть связаны с другими данными, хранящимися у правительства и наблюдателей от полиции и служб безопасности[3].

Очень часто среди ученых встречается мнение, что хранение метаданных не всегда может принести ожидаемый эффект. По мнению С.А. Филимонова это, в первую очередь, связано с тем, что для совершения преступления при помощи компьютерной сети достаточно приобрести портативное средство спутниковой связи. Время, в течение которого совершается этот вид преступлений, может занимать менее одной минуты, и преступник не ограничен в выборе страны, на территории которой он это устройство будет использовать. У правоохранительных

---

[1] Regulation of Investigatory Powers Act 2000 [Электронный ресурс]. – URL: https://www.legislation.gov.uk/ukpga/2000/23/contents (дата обращения: 08.02.2025).

[2] Перехват данных: кто, где и как [Электронный ресурс]. – URL: http://www.nestor.minsk.by/sr/2007/01/sr70102.html (дата обращения: 24.01.2025).

[3] John Lettice Gatso 2: rollout of UK's '24x7 vehicle movement database' begins [Электронный ресурс]. – URL: https://www.theregister.co.uk/2005/11/15/vehicle_movement_database (дата обращения: 19.02.2025).

органов на поиск и привлечение к уголовной ответственности такого лица, как правило, уходит значительное количество времени, в течение которого преступник имеет реальную возможность уничтожить следы преступления, чем затруднить или сделать невозможным привлечение его к уголовной ответственности[1]. Здесь также стоит добавить, что, если провайдер и сохранит метаданные о действиях пользователя в компьютерной сети, то идентифицировать этого пользователя благодаря только этим данным не удастся.

Такой пользователь для доступа в Интернет может использовать, например, бесплатные и открытые для свободного доступа Wi-Fi точки доступа. На лицо не отрегулированная проблема в сфере противодействия киберпреступности. Ее попыталось решить Королевство Дания (далее-Дания), которая 15 сентября 2007 года приняла закон (Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)). Согласно данному закону в Дании должен регистрироваться весь интернет-поток и сеансы между операторами и операторами и потребителями. В пункте 2.2.5 закона указано, что, помимо данных Интернета, поставщик должен сохранять данные, которые идентифицируют точное географическое или физическое местоположение точки доступа и идентификацию используемого коммуникационного оборудования[2].

Показателен в спектре рассуждения проблематики диссертационного исследования и пример Республики Беларусь. В данном государстве была изучена проблема бесплатных беспроводных сетей Wi-Fi, с помощью которых пользователь может подключиться к компьютерной сети не идентифицируя себя. Впоследствии был принят Указ Президента Республики Беларусь под № 350 «Об особенностях использования национального сегмента сети Интернет»[3], который

---

[1] Филимонов С.А. Некоторые проблемы борьбы с киберпреступностью как самых опасных транснациональных преступлений // APRIORI. Серия: Гуманитарные науки. – 2014. – № 1. – С. 29.

[2] Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) [Электронный ресурс]. – URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=2445#FN501 (дата обращения: 09.02.2025).

[3] Об особенностях использования национального сегмента сети Интернет: Указ Президента Республики Беларусь от 18 сентября 2019 г. № 350 [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь . – URL: http://president.gov.by/uploads/documents/2019/350uk.pdf (дата обращения: 14.02.2025).

обязал собственников пунктов коллективного пользования интернет-услугами или уполномоченных ими лиц осуществлять идентификацию таких пользователей в этих пунктах, учет и хранение персональных данных о них в течении года, а также сведений об интернет-услугах, оказанных пунктами их коллективного пользования. Под пунктами коллективного пользования интернет-услугами понимаются компьютерные клубы, интернет-кафе, домашние сети, другие места, в которых обеспечивается коллективный доступ пользователей к сети Интернет. Также в Указе под пользователем интернет-услуг понимается физическое или юридическое лицо, использующее информационные сети, системы и ресурсы сети Интернет.

По данному нормативному акту хранение сведений должно осуществляться в течение одного года со дня предоставления интернет-услуг. Сведения об абонентских устройствах, персональные данные пользователей Интернет-услугами в пунктах их коллективного пользования, а также сведения об оказанных интернет-услугах предоставляются поставщиками этих услуг, собственниками пунктов коллективного пользования таких услуг или уполномоченными ими лицами по требованию органов, осуществляющих оперативно-розыскную деятельность, органов прокуратуры и предварительного расследования, органов Комитета государственного контроля, налоговых органов, судов в порядке, установленном законодательными актами.

Стоит обратить внимание еще на один аспект анализируемой проблематики. Помимо метаданных, интерес представляют и данные, которые шифруются и передаются скрытно. Провайдеры не имеют возможности масштабно сохранять такие данные параллельно с метаданными. И чтобы получить такие данные, необходимо или иметь авторизированный доступ, где заходить под логином и паролем на конкретную пользовательскую страницу сайта, или полный административный доступ к базам данных сайта.

Германия осознала необходимость разрешения указанной проблемы одной из первых. 4 января 2016 года она приняла ФЗ «О сохранении данных» (Data Retention Act). Закон призван обеспечить правоохранительные органы электронными

данными для борьбы с «серьезными преступлениями» и требует, чтобы общественные телекоммуникационные и интернет-провайдеры сохраняли различные записи о деталях звонков, включая номера телефонов, дату и время телефонных звонков и текстов, где также упоминается о содержании текстовых сообщений и / или сотовые вызовы – местоположения участников вызова. Кроме того, интернет-провайдеры должны хранить пользовательские метаданные, такие как IP-адреса, номера портов, а также дату и время доступа в Интернет. Закон также обязывает поставщиков хранить детали звонков и метаданные в течение 10 недель и данные о местоположении сотового телефона в течение 4-х недель. В ответ на вопросы конфиденциальности и защиты данных Закон содержит обширные технические требования к тому, как поставщики хранят данные[1].

Обратим внимание в этом плане на опыт США. В законодательный орган США были представлены два законопроекта – S.436 и HR1076, названные как законы «О безопасности в Интернете», где прописано, что Интернет и хостинг -провайдеры обязаны в течение не менее двух лет сохранять весть трафик и другую информацию, относящуюся к пользователю, а также временно назначенный ему сетевой адрес.

Указанный законопроект «О безопасности в Интернете» должен был применяться не только к компаниям AT & T, Comcast, Verizon и т. д., но и к десяткам миллионов домов с точками доступа Wi-Fi или проводными маршрутизаторами, которые используют стандартный метод динамического назначения временных адресов. «Каждый человек должен хранить такую информацию», – говорит Альберт Гидари, партнер юридической фирмы Perkins Coie в Сиэтле, специализирующейся в области электронного законодательства о конфиденциальности. По его утверждению это должно касаться не только общедоступных точек доступа к Wi-Fi, но и защищенных паролем, и применяться к отдельным лицам, малым предприятиям, крупным корпорациям, библиотекам,

[1] German Data Retention Act Signed Into Law [Электронный ресурс]. – URL: http://www.winston.com/en/privacy-law-corner/new-german-data-retention-law-expected-to-take-effect-soon.html (дата обращения: 14.02.2025).

школам, университетам и даже государственным учреждениям[1].

По поводу данного закона было много замечаний и возражений, где, например, высказывалось мнение о том, что ведение журнала данных может быть отключено или полностью удалено на устройстве злоумышленником. Ведение журнала должно проверяться, но кто и в какие сроки должен это делать, в законе не было указано[2].

Таким образом, граждане в США все чаще представляют Интернет как место, сравнительно свободное от цензуры и технической фильтрации, однако в реалии контроль в стране очень жесткий. Помимо того, что законодатели США установили нормы, при помощи которых возможно ограничить доступ их граждан к информации и ее распространению, так и власти этой страны пытаются постоянно оказывать давление на провайдеров в части контроля содержания, изъятия или фильтрации в сети. Несмотря на то, что законодательные инициативы широко обсуждаются, отдельные меры могут быть непрозрачными[3].

Следует заметить, в США данные о пользователе не считаются персональными данными. Это связанно с тем, что в отличие от большинства ведущих европейских стран, в Соединенных Штатах Америки до сих пор отсутствует общее законодательство о персональных данных[4].

Наверное, по этой причине юристы Google приводят пример: «Отправка электронного письма через веб-сервис – это то же самое, как если бы вы воспользовались обычной почтой. Когда вы кидаете письмо в почтовый ящик, вы знаете, что сотрудники почты прочтут адрес на конверте для того, чтобы доставить письмо куда надо. Но вы не рассчитываете, что они вскроют конверт, чтобы

---

[1] Bill proposes ISPs, Wi-Fi keep logs for police [Электронный ресурс]. – URL: http://edition.cnn.com/2009/TECH/02/20/internet.records.bill/index.html (дата обращения: 08.02.2025).

[2] Bills S.436 and H.R. 1076, Their to protect the children!" No, it's not and we know it fucktard [Электронный ресурс]. – URL: https://krypt3ia.wordpress.com/2009/02/21/bills-s436-and-hr-1076-their-to-protect-the-children-no-its-not-and-we-know-it-fucktard/ (дата обращения: 25.01.2025).

[3] Лоскутов И.Ю. Сравнительный анализ международных норм законодательного регулирования Интернета в различных странах (2008 год) [Электронный ресурс]. – URL: http://www.zakon.kz/221107-sravnitelnyjj-analiz-mezhdunarodnykh.html (дата обращения: 28.01.2025).

[4] Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ - Scientific Journal of KubSAU. – 2015. – № 110. – С. 879.

прочесть содержимое», – отметил Симпсон[1].

США в настоящее время не имеют обязательного законодательства о сохранении данных**.** Однако, если поставщики электронных коммуникаций или удаленных вычислительных услуг хранят электронные сообщения или сообщения о связи, правительство может получить доступ к сохраненным данным в соответствии с Законом «О сохраненной связи» (Stored Communications Act), принятым в соответствии с Законом «О конфиденциальности электронных сообщений» в 1986 году. SCA также устанавливает обязательное сохранение данных, при котором провайдеры должны сохранять данные в течение 180 дней по запросу правительства[2].

Различные агентства США осуществляют добровольное сохранение компьютерных данных, практикуемое многими коммерческими организациями США, используя для этих целей различные базы данных. Общеизвестно, что Amazon сохраняет все возможные данные о транзакциях с клиентами. В свою очередь Google также сохраняет транзакции и поисковые запросы. Указанные компании базируются в США, чем активно пользуется Федеральное бюро расследований (далее – ФБР), получая доступ к такой информации посредством «Письма национальной безопасности (NSL)». По официальным данным компании Google только за 2024 год в компанию на предоставление пользовательских данных было сделано 236 520 NSL запросов, а доля запросов, по которым были предоставлены какие-либо данные, составляет в среднем 82 %[3].

Например, также известно, что Агентство национальной безопасности (далее – АНБ) США в специально разработанной базе данных MARINA регистрирует и хранит метаданные, полученные из сети Интернет, в течение года. Для записи SMS и различных текстовых сообщений АНБ использует базу данных, получившую название DISHFIRE. При этом оно руководствуется IV поправкой к Конституции

---

[1] Пользователи Gmail могут не рассчитывать на тайну переписки [Электронный ресурс]. – URL: http://www.cnews.ru/news/top/google_polzovateli_gmail_mogut_ne (дата обращения: 18.02.2025).

[2] 18 U.S. Code § 2704 - Backup preservation [Электронный ресурс]. – URL: https://www.law.cornell.edu/uscode/text/18/2704 (дата обращения: 13.02.2025).

[3] Запросы личной информации в Google [Электронный ресурс] // Отчет о доступности сервисов и данных Google. – URL: https://transparencyreport.google.com/user-data/overview?hl=ru (дата обращения: 13.02.2025).

США, где прописано, что прослушивание телефонных переговоров приравнивается по своим юридическим последствиям к обыску и осуществляется на основании ордера, то есть под контролем судебной власти.

В США с 1968 года производить прослушивание телефонных переговоров можно по разрешению (ордеру) суда и не более 30 суток. Возбуждение ходатайства о выдаче ордера осуществляется только прокурором на основе заявления сотрудника правоприменительного органа, ведущего расследование. При этом необходимо указать: конкретное преступление (готовящееся, совершенное или совершаемое), по которому предполагается проводить прослушивание; лицо, переговоры которого предполагается прослушивать; аргументы, обосновывающие необходимость прослушивания и характер переговоров[1].

Добавим, что после террористического акта 11 сентября 2001 года 24 октября этого же года в США был принят Акт «О сплочении и укреплении Америки путём обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» который, сокращенно назывался «Патриотический акт». В целях дальнейшего предотвращения действий террористического характера Акт наделил полицию США, спецслужбы и разведку определенными полномочиями, направленными на контроль за деятельностью граждан, путем прослушивания и получения информации об интернет-активности. Интересные статьи, связанные с получением информации из компьютерной сети, указаны в секциях 215, 216 данного Акта.

Так, секция 215, носящая название «Доступ к записям и другим предметам в соответствии с Законом о надзоре за внешней разведкой», предоставляет правоохранительным органам США право на получение различной информации, которая, по их мнению, станет значимой в процессе проведении антитеррористических расследований, и даже тогда, когда сами данные не будут иметь прямой связи с террористами. Также секция 215 освобождает сотрудников, в чьем производстве находятся дела по терроризму, от необходимости соблюдения

[1] Карпычев В.Ю., Немкова Н.А. Мировой опыт правового регулирования оперативных мероприятий на сетях связи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2010. – № 2(13). – С. 173.

процедуры получения ордера на обыск или получение информации, где нужно доказать обоснованность подозрений против человека.

В секции 216 Акта прописаны правила, по которым запросы данных, связанных с антитеррористической деятельностью NSL, могут не содержать имени конкретного человека и перечня конкретной информации, требующиеся властям[1]. Поэтому, благодаря этому закону, правоохранительные органы могут осуществлять массовое получение данных, проходящих через Глобальную сеть, относительно как одного человека, так и группы людей даже без причастности последних к террористической деятельности[2].

Издание Washington Post (Reuters) опубликовало информацию о том, что Американский федеральный апелляционный суд поддержал правила, которые позволяют ФБР тайно запрашивать данные, связанные с наблюдением за клиентами, в компании связи. NSL не требуют указания цели и ордера для получения данных[3]. ФБР также может получать в соответствии NSL информацию о людях, которые не совершили каких-либо преступлений. Десятки тысяч NSL поступают ежегодно в компании Интернет и мобильной связи, а некоторые из них на неопределенный срок.

Центральное разведывательное управление (далее – ЦРУ) США не остановилось на достигнутом. Так 7 марта 2017 года произошло недооцененное экспертами событие: Wikileaks начала публикацию информации под кодовым названием Vault 7, содержащей подробности работы ЦРУ. В документах раскрываются сведения о наличии у спецслужб готовых эксплойтов для множества 0day-уязвимостей в различном программном обеспечении. К примеру, именно через такие 0day-уязвимости ЦРУ компрометирует мобильные устройства и перехватывает сообщения популярных мессенджеров («WhatsApp», «Signal», «Telegram», «Weibo», «Confide» и «Clockman»): спецслужбы не взламывают шифрование, а компрометируют сам девайс, на котором установлено приложение.

[1] USA Patriot Act (H.R. 3162) https://epic.org/privacy/terrorism/hr3162.html (дата обращения: 09.02.2025).

[2] Большой и заботливый брат [Электронный ресурс]. – URL: https://tjournal.ru/p/google-for-surveillance-reform (дата обращения: 22.02.2025).

[3] U.S. appeals court upholds gag orders on FBI data surveillance [Электронный ресурс]. – URL: http://www.reuters.com/article/us-usa-surveillance-idUSKBN1A21XJ (дата обращения: 25.01.2025).

Только в операционной системе iOS ЦРУ сумели найти семь различных багов и создали для них как минимум четырнадцать эксплойтов. 23 марта на Wikileaks был также опубликован ряд проектов ЦРУ, при помощи которых спецслужбы заражают технику Apple вирусом, который продолжает «жить» даже после переустановки операционной системы. Например, одним из таких вирусов является Night-Skies, который предназначен для заражения iPhone и устанавливается на чистые устройства, только вышедшие с конвейеров фабрик. Становится очевидным, что ЦРУ давно имеет физическую возможность внедряться в логистическую цепочку Apple, заражая устройства прямо «из коробки»[1].

Австралия тоже пытается эффективно противодействовать киберпреступности. С целью более серьезного обеспечения расследования незаконной деятельности в Интернете, данная страна приняла ряд нормативно-правовых актов:

1) Закон о телекоммуникации (перехват и доступ) 1979 года (Telecommunications (Interception and Access) Act). Этот закон с поправками, внесенными в июне 2006 года, запрещает перехват телекоммуникаций или запрет доступа без предварительного уведомления как отправителя, так и получателя, любого физического или юридического лица, за исключением случаев, таких, как установка и обслуживание телекоммуникационного оборудования. Он также устанавливает процедуру под контролем Генерального прокурора, в соответствии с которой правоохранительные органы могут получить доступ к частным сообщениям австралийских компаний, которые работают в важных отраслях экономики, и которым разрешено следить за интернет-перепиской своих сотрудников. Австралийское правительство таким образом намерено бороться с терроризмом;

2) Закон о надзоре за устройствами (Surveillance Devices Act) 2007 года. В соответствии с ним полиция Австралии получает официальное разрешение устанавливать на компьютеры подозреваемых преступников вирусы («троянских коней») или шпионы (spyware) при помощи упомянутого в законе «устройства

[1] Мария Нефедова Публикация VAULT 7 // Журнал «Хакер» № 218 март 2017.

наблюдения за данными». Под последним понимается любое устройство или программа, способные использоваться для записи или мониторинга ввода информации и вывода информации с компьютера. В секции 17 закона сказано, что сотрудник правоохранительных органов может подать заявку на выдачу ордера на устройство наблюдения. Интерес здесь представляет и секция 18, где отмечено, что заявление сотрудником правоохранительных органов может быть сделано по телефону, факсу, электронной почте или любым другим средством связи[1].

В русле отмеченного следует упомянуть и введенный в действие с 2015 года австралийский закон**,** связанный с сохранением данных – Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. Данный нормативный источник требует от провайдеров телекоммуникационных услуг и интернет-провайдеров сохранения метаданных в течение 2-х лет. Соответствующие данные будут доступны без ордера и могут использоваться для целевого обмена файлами.

Согласно закону, правом запрашивать и получать доступ к данным, которые хранят поставщики услуг, наделены 22 государственных органа, включая правоохранительные органы и ведомства, уполномоченные в области обеспечения национальной безопасности. При этом для указанных ведомств предусматривается механизм доступа к данным, не требующий получения и предоставления судебного ордера[2].

Обращает на себя внимание и австралийский Закон о государственном контроле над содержимым сети Интернет, известный как «Broadcasting Services Amendment (Online Services) Act»[3], вступивший в действие с 1 января 2000 года. Закон предусматривает введение рейтинговой системы (похожей на существующую аналогичную систему для кинофильмов), классифицирующей сетевой контент по степени его «порнографичности», как это определено по Акту

[1] Surveillance devices act № 64 of 2007 [Электронный ресурс]. – URL: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/sda2007210/ (дата обращения: 14.02.2025).

[2] Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 [Электронный ресурс]. – URL: https://www.legislation.gov.au/Details/C2015A00039 (дата обращения: 13.02.2025).

[3] Broadcasting Services Amendment (Online Services) Act 1999 16.07.1999 No. 90 [Электронный ресурс]. – URL: https://www.legislation.gov.au/Details/C2004A00484 (дата обращения: 08.02.2025).

Британского Содружества «О классификации публикаций, фильмов и компьютерных игр» 1995 года. По закону интернет-провайдеры обязуются в 24 часа удалять материалы, классифицированные X (Sexually Explicit) или RC (Refused Classification – детская порнография, фетиш, подробные инструкция по совершению преступлений, и так далее). В случае несоблюдения провайдером указанного требования на него может быть возложена обязанность уплаты специального штрафа, сумма которого может достигать 27 000 австралийских долларов за день неисполнения предписания[1].

Французская Республика (далее-Франция), как представитель Европейского Союза, сегодня идет по пути четкого государственного определения механизмов функционирования сети Интернет. В данном государстве разработано и введено в действие законодательство, которое обязывает провайдеров сообщать сведения об авторах сайтов любому заинтересованному третьему лицу под страхом тюрьмы. Во Франции также установлена обязательная регистрация владельцев всех веб-сайтов страны, дополнительно введены меры уголовного наказания и для тех провайдеров, которые предоставляют хостинг не идентифицированным пользователям. Указанные законодательные меры направлены, прежде всего, на устранение анонимности авторов сайтов, то есть посредством данных мер вводится автоцензура на уровне провайдера.

На сегодняшний день провайдер во Франции отвечает за всех авторов своего сервера. Но следует также принимать во внимание и положения французского закона «О доверии в цифровой экономике» от 21 июня 2004 г. Согласно указанному нормативно-правовому акту субъект, осуществляющий автоматическое переходное и временное хранение информации, не несет юридической ответственности за хранение такой информации в случае, когда: единственной целью этого субъекта является эффективная передача данных заказчикам услуг; интернет-провайдер не осуществляет изменение содержания информации, придерживается установленных требований по осуществлению доступа к

[1] Законодательство Республики Казахстан – URL: https://www.zakon.kz/221107-sravnitelnyjj-analiz-mezhdunarodnykh.html (дата обращения: 02.02.2025).

информации и ее обновлению. Провайдер также обязан в случае подтверждения факта противоречия законным требованиям содержания информации принимать незамедлительно меры по удалению такой информации или закрытию доступа к ней.

Как видим, осознание необходимости принятия более кардинальных мер законодательного характера в деле противодействия киберпреступности присутствует у многих современных государств. Многие из них пытаются законодательно разрешить обозначенную проблему. Но иногда получается, что отдельные государства принимают только паллиативные меры. Что, конечно же, не приносит ожидаемых результатов.

Так, в частности, одной из причин существования киберпреступности, является анонимность пользователя. И лишь в некоторых странах эта проблема решается определенным образом, преимущественно с помощью административных мер. Например, в Итальянской Республике (далее-Италия) после известного теракта 11.04.2004 г. все пользователи общественных точек доступа к Интернету должны предъявлять паспорт или идентификационную карту. В Китайской Народной Республике (далее-Китай) с 2011 г. с целью недопущения клеветы, недобросовестной рекламы и мошенничества при регистрации на сайтах, в социальных сетях также необходимо вводить паспортные данные. Конечно же, подобные меры среди населения стран были не популярными, хотя от их применения эффект был ощутимым – резко пошел на убыль уровень киберпреступности в социальных сетях[1].

Обратим также внимание на то, что в различных государствах по-разному разрешается и вопрос о сохранении и доступе к данным. Так, например, немецкий законодатель выдвигает особые требования к провайдеру за содержание предоставляемых им услуг в случае, если они знакомы с содержанием. В этом случае при наличии технических возможностей информация блокируется, но с обязательным обоснованием таких действий. При этом провайдеру в обязательной

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – М., 2016. – С. 55.

форме предписывается блокирование противоречащей закону информации. Кроме этого, закон требует от провайдера отвечать и за информацию, предоставляемую пользователю непосредственно им самим. Но вместе с тем, законодатель освобождает провайдеров от ответственности, если пользователь, воспользовавшись его услугами, получил доступ к данным, не принадлежащим провайдеру. Так, к примеру, в Федеральном Законе Германии о телекоммуникационных услугах (Teledienstegesetz, TDG) отмечается, что провайдеры, согласно общим нормам, отвечают за собственное содержание, которое они сделали доступным для использования. Они также несут ответственность за данные третьих лиц, когда делают их доступными или, когда им известна передаваемая информация, которую они могут на законном основании заблокировать.

В подобных случаях имеет место на практике вышеописанная ситуация, когда собственника ЭВМ, выполняющей функции «сервера», нельзя отождествлять с обладателем права на нематериальные объекты, размещенные на таком компьютере. Если же применять конструкцию «документированной информации», декларирующей единство материального носителя информации и самой информации, то следовало бы считать провайдера собственником не только ЭВМ, но и собственником в целом всей «документированной информации», включая сервер, на котором временно размещается информация, и саму информацию. Следовательно, в таком случае провайдер считался бы в буквальном смысле собственником личных тайн своих клиентов-граждан и собственником объектов авторского права, которые размещены на сервере[1].

Если говорить о Королевстве Испания (далее- Испания), то там предписано каждому коммерческому сайту пройти регистрацию в качестве магазина. Для некоммерческих сайтов, регистрацию проходить не нужно. Но все же владелец обязан указать на страницах своего сайта имя, адрес и личный код. Особые требования предъявляются к провайдерам, связанным с деятельностью

[1] Огородов Д.В. Правовые отношения в информационной сфере. дис. … канд. юрид. наук: 12.00.09 / Огородов Дмитрий Владимирович. – М., 2002. – С. 192.

зарубежных сайтов. В случае выявления на них информации, угрожающей национальной безопасности государства, доступ к последним блокируется.

Что касается Великобритании, то в ней в 2001 году создано Национальное отделение по борьбе с преступлениями в области высоких технологий (The National High-Tech Crime Unit, NHTCU). Оно наделено правом фильтрации контента интернет-ресурсов. NHTCU также тесно взаимодействует с телекоммуникационными службами и собирает соответствующую информацию. При этом нужно понимать, что британский Закон о защите данных (The Data Protection Act) накладывает ряд определенных ограничений на сбор телекоммуникационными компаниями данных о пользователях.

Существует в Великобритании и Фонд наблюдения за Интернетом (Internet Watch Foundation, IWF). Он тесно сотрудничает с Интерполом, полицией и подразделением по борьбе с преступлениями. Данный фонд активно пытается вести борьбу с интернет-педофилией. Соответствующую информацию ему предоставляют провайдеры и телекоммуникационные компании, а также организации по защите детей[1].

Интересная ситуация складывается в Украине, где с 18.11.2003 г. действует Закон «О телекоммуникациях». В п. 4 ст. 39 данного нормативного акта указывается, что «Операторы телекоммуникаций обязаны за собственные средства устанавливать на своих телекоммуникационных сетях технические средства, необходимые для осуществления уполномоченными органами оперативно-розыскных мероприятий, и обеспечивать функционирование этих технических средств, а также в пределах своих полномочий содействовать проведению оперативно-розыскных мероприятий и недопущению разглашения организационных и тактических приемов их проведения. Операторы телекоммуникаций обязаны обеспечивать защиту указанных технических средств от несанкционированного доступа»[2].

[1] Protection of Children Act 1978 [Электронный ресурс]. URL: https://www.legislation.gov.uk/ukpga/1978/37 (дата обращения: 14.02.2025).

[2] О телекоммуникациях: Закон Украины от 18 ноября 2003 № 1280-IV [Электронный ресурс] // Официальный сайт Верховной Рады Украины. – URL: http://www.Zakon.rada.gov.ua (дата обращения: 11.02.2025).

Анализ украинского законодательства показывает, что при обнаружении информации, которая является поводом для начала оперативно-розыскной деятельности, возникают проблемы при поиске и установлении лиц, причастных к этой информации, в связи с неурегулированием в этом законе срока хранения информации и отсутствием четко указанного перечня информации, которую необходимо хранить для предоставления ОВД. Это также связанно с основаниями для проведения оперативно-розыскной деятельности, указанными в ст. 6 Закона Украины «Об оперативно-розыскной деятельности», а именно: «…основания могут содержаться в заявлениях, сообщениях граждан, должностных лиц, общественных организаций, средств массовой информации, в письменных поручениях и постановлениях следователя, указаниях прокурора, постановлениях суда по уголовным делам, находящимся в его производстве, материалах органов дознания, других правоохранительных органов, в запросах и сообщениях правоохранительных органов других государств и международных правоохранительных организаций, а также запросах полномочных государственных органов, учреждений и организаций, определенных Кабинетом Министров Украины, о проверке лиц в связи с их допуском к государственной тайне и к работе с ядерными материалами и на ядерных установках»[1].

Согласно ст.1 закона Украины «О печатных средствах массовой информации (прессе) в Украине» под печатными средствами массовой информации (прессой) в Украине понимаются периодические и регулярные издания, выходящие под постоянным названием, с периодичностью один и более номеров (выпусков) в течение года на основании свидетельства о государственной регистрации[2]. Если проанализировать понятия «средства массового информации» и «Интернет» по украинскому законодательству, то можно сделать вывод, что Интернет не является средством массовой информации, в связи с чем не может информация, полученная

[1] Об оперативно-розыскной деятельности: Закон Украины от 18 февраля 1992 года № 2135-XII [Электронный ресурс] // Официальный сайт Верховной Рады Украины – URL: http://zakon2.rada.gov.ua/laws/show/2135-12/page2 (дата обращения: 11.02.2025).

[2] О печатных средствах массовой информации (печати) в Украине: Закон Украины № 2782-XII от 16 ноября 1992 [Электронный ресурс] // Официальный сайт Верховной Рады Украины. – URL: http://zakon3.rada.gov.ua/laws/show/2782-12 (дата обращения: 11.02.2025).

из Глобальной сети Интернет, быть основанием для проведения оперативно-розыскной деятельности.

Наряду с иностранными государствами предприняты попытки получения контроля над Глобальной сетью и в Российской Федерации**.** В частности, 7 июля 2016 Президент РФ В.В. Путин подписал Федеральный закон «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», который разработали депутат И. Яровая и сенатор В. Озеров. Указанный нормативно-правовой акт, получивший в России название «Пакет антитеррористических поправок Яровой» (далее – поправки Яровой), дополнил ст. 6 ФЗ «Об оперативно-розыскной деятельности» новым ОРМ – «Получение компьютерной информации». Однако, за исключением того, что данное мероприятие должно проводиться по решению суда, но, в каких случаях и как должно фиксироваться, не разъяснено[1].

Обратим также внимание на то, что с 1 июля 2018 на основании ст. 13 поправок Яровой в ст. 64 ФЗ «О связи» от 07.07.2003 г, прописано, что все операторы связи обязаны хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение 3-х лет с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до 6 месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Указывается также на необходимость взаимодействия с органами,

[1] 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»: Федеральный закон от 06 июля 2016 № 374-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

осуществляющими оперативно-розыскную деятельность, при проведении оперативно-розыскных мероприятий с использованием сетей связи. В частности, операторы обязаны предоставлять накопленную информацию о пользователях и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач[1].

Помимо ФЗ «О связи» в соответствии со ст. 15 поправок Яровой были внесены изменения и в статью 10.1 Федерального закона от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», где аналогичные сроки хранения коснулись организаторов распространения информации в сети Интернет, а также в п. 3.1 – теперь закреплено обязательство организатора распространения информации в сети Интернет при кодирования трафика представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для его декодирования[2].

Еще одним нововведением поправок Яровой стали корректировки ч. 4 ст. 15 ФЗ «О Федеральной службе безопасности» и ч. 3. ст. 6 ФЗ «О внешней разведке», которые позволяют теперь федеральному органу исполнительной власти и, соответственно, службе внешней разведки РФ получать на безвозмездной основе от государственных органов и государственных внебюджетных фондов необходимые для выполнения возложенных на них обязанностей информационные системы и (или) базы данных, в том числе и путем получения возможности удаленного доступа к ним[3]. Напомним, что в ФЗ «Об оперативно-розыскной деятельности» не прописаны возможности для соответствующих государственных органов осуществлять удаленный доступ к базам данных, что, на наш взгляд, является существенным законодательным пробелом.

Бесспорно, данные операторов связи и организаторов распространения

---

[1] О связи: Федеральный закон от 07 июля 2003 № 126-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.01.2025).

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.01.2025).

[3] О Федеральной службе безопасности: Федеральный закон от 03 апреля 1995 № 40-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025); О внешней разведке: Федеральный закон от 10 января 1996 N 5-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

информации в сети Интернет могут содержать сведения о следах противоправной деятельности пользователей. Анализ таких данных даст возможность не только выявить сведения о месте совершаемого противозаконного действии пользователя, но также выявить ту информацию, которая может указывать на нераскрытые преступления. В спектре необходимости практического разрешения задач ОРД остается открытым вопрос касательно установления оптимальных сроков хранения соответствующих данных. На необходимость хранения данных провайдерами в течении 10 дней указывают 3% опрошенных оперативных сотрудников. При этом 30% респондентов считают, что компьютерную информацию провайдеры должны хранить 1 месяц, 55 % – от 3 до 6 месяцев, 10% – от 6 до 12 месяцев и 2 % полагают, что необходимо хранить более 1 года[1].

Необходимо также определить на нормативном уровне, в каком виде эти данные будут храниться и предоставляться. Сама же обязанность по реализации этой функции безусловно ляжет на плечи операторов связи и провайдеров, которые будут нести в соответствии с этим существенные финансовые потери.

Не стоит забывать, что потенциал сети далеко не исчерпан и, как половинчатые меры, так и чрезмерные усилия по законодательной регламентации Интернет-пространства могут становиться серьезным препятствием на пути его развития. Поэтому действия при работе с данными должны не только не нарушать конституционные права и свободы граждан, но способствовать оперативному выявлению лиц, склонных к использованию компьютерной информации в преступных целях.

На наш взгляд, Россия должна использовать в деле противодействия преступлений в сфере информационных технологий весь позитивный опыт, который накоплен зарубежными странами. В частности, в Российской Федерации можно было бы создать более благоприятные условия для противодействия киберпреступности, а именно – упростить механизм получения компьютерной информации, как это, например, реализовано в Австралии. В этой стране данные могут быть получены оперативным путем по средствам связи, а также при помощи

[1] См.: Приложение № 1. Опросный лист.

различных специализированных программ и устройств. Стоит также изменить подход к хранению компьютерной информации в целесообразных временных рамках и только в отношении лиц, представляющих оперативный интерес (например, как NSL - запросы в США).

С учетом отмеченного, можно заявить о том, что ФЗ «Об оперативно-розыскной деятельности» требует внесения дополнений о закреплении в нем возможности для правоохранительных органов осуществлять удаленный доступ к компьютерной информации, имеющей значение для расследования. В ст. 6 ФЗ «Об оперативно-розыскной деятельности» следует регламентировать, 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 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».

ГЛАВА 2. ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ПОЛУЧЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ЦЕЛЯХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 2.1. Особенности организации расследования преступлений с использованием компьютерной информации

Трансформация преступности неумолимо заставляет правоохранительные органы видоизменять поход к организации расследования преступлений, концентрировать внимание на оперативном реагировании с целью быстрого и полного их раскрытия, при этом постоянно повышая эффективность проведения первоначальных и последующих следственных действий, а также оперативно-розыскных мероприятий.

Положительных результатов в деле противодействия преступности можно достичь только в тех случаях, если деятельность служб и подразделений органов внутренних дел по раскрытию ими преступлений будет правильно и эффективно организована, а также направлена на получение необходимой информации, где наиболее актуальной на сегодняшний день представляется компьютерная информация.

По утверждению некоторых ученых широкая распространенность и доступность информации для пользователей сети Интернет способствовала росту уровня преступности более чем в 20 раз[1]. Это также указывает на необходимость надлежащего организационного обеспечения задействования компьютерных технологий правоохранительными органами в расследовании преступлений. В свой черед, совершение преступлений с использованием современных компьютерных технологий не только усложняет расследование, но и создает ему существенное противодействие.

[1] Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 2-2. – С. 24.

В настоящее время достаточно большое количество преступлений совершается посредством компьютерной информации, которая используется в качестве как основного, так и вспомогательного источника информации. И даже в тех случаях, когда то или иное лицо пытается максимально исключить использование в своей деятельности компьютерные технологии, это не означает, что компьютерная информации о лице будет полностью отсутствовать. Здесь подразумевается, что лицо, причастное к совершению преступления, могло даже и не знать, что следы его противоправной деятельности оказались зафиксированы при помощи компьютерных технологий и хранятся в виде данных на различных ресурсах. В свою очередь, при правильной организации деятельности правоохранительных органов компьютерная информация может быть получена в любой момент, на любом этапе расследования и стать не только ориентирующей, но и процессуально значимой, т.е. иметь доказательственное значение.

Проведенный анализ ситуации, связанной с получением компьютерной информации, позволяет сделать вывод о необходимости разработки ряда вопросов, связанных с организацией работы следователя по поиску компьютерной информации, имеющей значение для расследования преступлений. Вызвано это также тем, что существующие научные работы, затрагивающие вопрос использования правоохранительными органами компьютерной информации, недостаточно углубленно освещают вопросы организации расследований преступных деяний. Учеными не всегда уделяется должное внимание анализу вопросов получения компьютерной информации в процессе расследования преступлений, совершаемых в реальном мире, где отсутствуют четкие векторы поиска нужного информационного источника (технического средства, ресурса), информация из которого может существенно повлиять на ход расследования. Данное направление необходимо и дальше развивать и научно обосновывать соответствующие рекомендации практического характера для процесса организации как расследования определенного вида преступлений, так и расследования преступлений в общем, поскольку сущность самого расследования, - как обоснованно отмечает В.Д. Зеленский, - состоит в том, что оно представляет

собой ту специфическую социальную деятельность по поиску, обнаружению, получению, исследованию и оценке доказательств, которая позволяет привести к установлению подлинных обстоятельств преступления[1].

С учетом развития современных информационных технологий одним из значимых видов такой деятельности и в тоже время специфическим направлением в расследовании преступления справедливо можно считать поиск и получение компьютерной информации.

Расследование преступлений, это не только сложная, но и комплексная, а также многоплановая деятельность, от эффективности которой зависит успех борьбы с преступностью и поэтому необходимо постоянно совершенствовать организационный процесс расследования.

Грамотная организация процесса расследования, в том числе с использованием компьютерной информации, а именно, упорядочение путем выявления основных элементов структуры, построения умственной модели предстоящей деятельности, создание условий для ее качественного производства и руководства расследованием[2], непременно принесет положительный результат.

Как правило, расследование преступлений осуществляется в условиях отсутствия достаточного объема полезной информации, дефицита времени, при постоянно меняющейся обстановке, нередко при противодействии преступника и других заинтересованных лиц. Поэтому в таких условиях очень трудно задействовать все имеющиеся информационные источники, в том числе содержащие компьютерную информацию. Более того, в силу различных факторов (обработка большого объема информации, различные форматы данных, а также множественные способы их хранения и передачи компьютерной информации), для большинства сотрудников правоохранительных органов является затруднительным правильная организация процесса расследования преступления. Это обуславливает выработку новых подходов к совершенствованию организации

[1] Зеленский В.Д. Теоретические вопросы организации расследования преступлений. Монография. – Краснодар: КубГАУ, 2011. – С. 6.

[2] Там же. – С. 59.

и планирования расследования преступлений с использованием компьютерной информации.

Обратим внимание на то, что расследование, как специфический вид социальной деятельности, имеет определенную структуру. В ряду основных структурных элементов большое значение отводится целям, как образующему и определяющему началу расследования[1]. Цель организационного процесса – определить его структурные элементы в их взаимосвязи[2].

Целеопределение – это интеллектуальный процесс, направленный на определение предмета расследования, то есть определение и конкретизацию обстоятельств, подлежащих установлению по делу, включая недостающие и промежуточные факты[3].

При получении компьютерной информации целью должно стать не хаотичное получение компьютерной информации, а ее полная фиксация всеми доступными законными методами и средствами. Следователю целесообразно первоначально стремиться к получению и фиксации имеющейся информации о субъектах преступления (анкетные данные, место работы), далее необходимо установить сведения о событиях и фактах, которые могут способствовать раскрытию преступлений (произвести анализ телефонных звонков, видео с камер видеонаблюдения, информации об интернет - активности лица и т.п.), учитывая при этом как доступность и законность получения такой информации, так и возможность придания ей процессуальной формы. Ставя цели в процессе расследования, следователь должен также учитывать, что целенаправленность, качество, результативность и законность деятельности в сфере уголовного судопроизводства могут быть реализованы с помощью использования организационных приемов, методов, средств и рекомендаций, которые

[1] Головин М. В. Проблемы целеопределения в расследовании: монография / М. В. Головин, Н. М. Шпак. – Краснодар: КубГАУ, 2014. – С. 3.

[2] Зеленский В.Д. Организационные функции субъектов расследования преступлений: монография / В.Д. Зеленский. – Краснодар: КубГАУ, 2005. – С. 15.

[3] Зеленский В.Д., Агеев Н.В. О структуре организационного процесса отдельного расследования // Вестник Самарского юридического института. – 2019. – № 3 (34). – С.43.

предоставляют широкие возможности для обеспечения эффективности работы правоохранительных органов[1].

В свою очередь следователь до момента начала получения компьютерной информации должен четко спланировать свои действия.

Анализируя следственную практику, Д.С. Свашенко приходит к выводу, что при расследовании преступлений следователь сталкивается с рядом процессуальных и криминалистических проблем, которые непосредственно связаны именно с планированием организации расследования преступлений[2]. Планируя будущее расследование, следователь должен не только использовать накопленные знания, представления, профессиональный опыт, но и получать внешнюю информацию, то есть такую, что поступает при изучении обстановки и обстоятельств расследуемого преступления[3].

Планирование расследования преступлений – это наиболее эффективный способ организации расследования по уголовному делу, включающий в себя сложную мыслительную деятельность уполномоченных субъектов на протяжении всего предварительного следствия, которая заключается в системе взаимосвязанных элементов по установлению цели и задач расследования, формированию версий, определению средств и методов их проверки, выраженная в письменной или графической формах[4]. Из данного понятия следует, что помимо мыслительной деятельности очевидным видится составление плана расследования. Мы убеждены, что в план расследования необходимо вписать отдельным пунктом получение компьютерной информации в соответствии с поставленными целями.

Для достижения положительного результата цель в расследовании преступления с использованием компьютерной информации должна быть напрямую связана как с планированием, так и с выдвижением следственных

---

[1] Можаева И.П. Криминалистическое учение об организации расследования преступлений: современное состояние и перспективы // Труды Академии управления МВД России. – 2015. – №. 4 (36). – С.82.

[2] Свашенко Д.С. Планирование расследования налоговых преступлений: дис. ... канд. юрид. наук / Сващенко Дмитрий Сергеевич. – Краснодар, 2016. – С. 18.

[3] Соя-Серко Л.А. Программирование и творчество в деятельности следователя // Проблемы предварительного следствия в уголовном судопроизводстве. - М.: Изд-во Всесоюзного ин-та по изучению причин и разработке мер предупреждения преступности. – 1980. – С. 32.

[4] Курьянова Ю.Ю. К вопросу о понятии планирования расследования преступлений // Сибирский юридический вестник. – 2010. – №. 1. – С. 70.

версий. По мнению ученых Э.О. Самитова и С.Я. Казанцева, основанном на многочисленных криминалистических исследованиях, именно версии считаются основой планирования расследования[1], что объективно обуславливает необходимость построения следственных версий и недостаток информации[2].

Задействование компьютерных технологий в расследовании позволит нужную для планирования информацию сделать более полной и доступной одновременно многим следователям и тем самым значительно повысить эффективность расследования.

Н.В. Кручинина, Н.С. Туренко правомерно обращают внимание на то, что основанием для построения версии может служить любая информация, поступившая из любого источника как в стадии возбуждения уголовного дела, так и в стадии предварительного расследования[3].

Однако для того, чтобы получать компьютерную информацию, имеющую значение в процессе расследования, необходимо учитывать некоторые особенности ее установления в процессе расследования, а именно понимать, какие источники нужно задействовать, для чего стоит выдвинуть определенные версии.

В свой черед выдвижение версий и определение вопросов, подлежащих доказыванию, в условиях применения следователем компьютерных технологий имеют свои особенности. При применении компьютерных технологий следователю приходится иметь дело с информацией, зафиксированной в памяти различных технических устройств.

Учитывая, что основу организации расследования преступлений, в том числе и совершенной с использованием компьютерной информации, составляет планирование, осуществляемое исходя из криминалистических версий, стоит предложить несколько типовых версий, которые могут применяться следователями при расследовании преступлений, независимо от сложившейся следственной ситуации, в частности:

---

[1] Самитов Э.О., Казанцев С.Я. Типичные версии и планирование расследования истязаний // Вестник Московского университета МВД России, – 2016. – №. 4. – С. 209.

[2] Зеленский В.Д. О понятии и содержании организации расследования преступлений // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9, № 4. – С. 739.

[3] Кручинина Н.В., Туренко Н.С. Выдвижение и проверка версий // Законность. – 2006. – № 12 (866). – С. 33.

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.

Если есть первичные данные о совершенном преступлении, следователю стоит проверить наличие компьютерной информации, содержащейся в банках данных МВД, при помощи которых, в зависимости от имеющихся сведений, путем различных запросов может быть получена информация (анкетные данные) как о лице, в отношении которого совершено преступление, так и о лицах, которые могут быть причастны к совершению преступлений (криминальные связи потерпевшего). При работе с банками данных МВД следователь также может сравнить имеющиеся у него первичные сведения с информацией об аналогичных преступлениях, которая уже ранее была занесена в базы данных. Следователь может выяснить, задерживалось ли ранее лицо за совершение преступлений, наличие у лица судимости, находится ли оно в розыске, имеется ли в распоряжении лица оружие. Также интерес может представлять содержащаяся в банках данных информация о похищенном или утраченном имуществе, документах, оружии, транспортном средстве.

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

Если лицо, подозреваемое в совершении преступления, для реализации преступного умысла запрашивало информацию или работало с информацией на определенном ресурсе или сервере, то необходимо осуществить запрос владельцу такого ресурса касательно сохраненных данных о подозреваемом, а также получить информацию, связанную с его деятельностью[1]. Если лицо было пользователем сети

[1] Еремченко В.И., Зиновьева Н.С. Алгоритм использования электронного почтового ресурса как источника доказательственной информации // Вестник Краснодарского университета МВД России. – 2014. – № 3 (25). – С. 64.

Интернет, то стоит обратиться к провайдеру, предоставляющему услуги связи пользователю, с целью получения информации в виде ссылок о посещаемых им интернет - ресурсах. Особый интерес могут представлять ссылки на социальные сети, сервера электронных почтовых ящиков, «облака», мессенджеров, при этом стоит также воспользоваться различными поисковыми системами для поиска информации по анкетным данным пользователя. Если лицо сбывало имущество, добытое преступным путем, то необходимо воспользоваться досками объявлений, тематическими форумами. При наличии фотографии лица или предмета, следователю стоит воспользоваться специализированными сайтами и программным обеспечением, предназначенными для поиска по фотографии.

2. В зависимости от физического места нахождения информационного источника:

а) Интересующая компьютерная информация, имеющая значение для расследования преступления, содержится непосредственно на техническом средстве, принадлежащем лицу, причастному к совершению преступления.

Если техническое средство (например, мобильный телефон, HDD, SSD, флеш-накопитель, видеорегистратор, фотоаппарат, видеокамера, диктофон, экшен-камера), содержащее компьютерную информацию, имеющую значение для расследования преступления, находилось при свидетеле, потерпевшем, подозреваемом и источник информации был выявлен в ходе проведения следственных действий, а также известно, что источник мог использоваться как при совершении преступления, так и при подготовке к нему, то необходимо получить и зафиксировать информацию, которая находилась на этом устройстве. Если преступление совершено при помощи технических средств или известно, что на месте совершения преступления имеется специфическая техника, необходимо определить, какие технические и программные средства будут наиболее оптимальны при получении интересующей информации.

б) Интересующая компьютерная информация находится на технических средствах, не принадлежащих лицу, причастному к совершению преступления,

однако, при помощи которых мог быть зафиксирован факт совершения преступления в момент или после его совершения.

Если при свидетеле, потерпевшем, подозреваемом или на месте совершения преступления не находилось техническое средство, однако следователю может быть известно или следователь может предположить, что имеется техническое средство, при помощи которого могла быть зафиксирована информация о совершении преступления, то следователь должен принять меры для установления местонахождения технического средства (например, камер наблюдения, в том числе и скрытых или выяснить, хранится ли компьютерная информация еще где-то в виде резервных копий) с дальнейшим получением компьютерной информации. Здесь также необходимо побеспокоиться об изъятии оригинального электронного носителя, либо фиксировать файлы с записью события путем их копирования[1] *и подготовить для этих целей накопитель.*

в) Доступ к компьютерной информации осуществляется удаленно.

Если в учреждении или организации используется программное обеспечение, которое работает по принципу клиент-сервер (1-с бухгалтерия), то стоит предположить, что физические носители (сервера) с компьютерной информацией могут находиться на территории других государств или быть территориально распределенными. Здесь стоит выяснить топологию сети, произвести осмотр оборудования, при помощи которого осуществляется выход в Глобальную сеть. В случае установления, что компьютерная информация находится на удаленном оборудовании, стоит выяснить место нахождения технических средств, IP-адрес(а), какое программное обеспечение установлено, кто еще может иметь физический доступ к оборудованию, а также кто и при помощи какого программного обеспечения может настраивать его удаленно.

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

[1] Дуленко В.А., Бронфман Б.Е. К вопросу расследования преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. – 2016. – № 2 (72). – С. 47.

а) Компьютерная информация, представляющая интерес в расследовании, находится на поврежденном техническом средстве.

Если компьютерная информация находится на носителе, который в случае воздействия различных факторов поврежден или который пытались повредить физически, то следователю необходимо принять меры для его сохранности и постановки вопроса о восстановлении его работоспособности и доступе к компьютерной информации, которая может на нем храниться. Для этого следователь может направить испорченный источник экспертам для проведения компьютерных экспертиз.

б) Компьютерная информация находится на техническом средстве доступ, к которому защищен при помощи программных или аппаратных средств.

Если имеется возможность получить доступ к такому устройству, то при наличии соответствующих знаний или с участием специалиста целесообразно произвести самостоятельный обход защиты на месте, например, если устройство заблокировано при помощи графического ключа и на экране остался след от его ввода. При проверке данной версии следователь должен поставить вопрос о привлечении специалиста и выяснить, может ли последний оказать консультационную помощь для осуществления доступа к устройству на месте? Здесь нужно не допустить уничтожение или изменение первоначального состояния информации, что приведет к признанию недопустимыми полученные доказательства. В случае, если следователь не умеет или затрудняется совершить обход (взлом) защиты, то ему необходимо попытаться выяснить способы, при помощи которых была выставлена защита, какие программные или аппаратные средства были использованы, использовалось ли шифрование данных и направить носитель компьютерной информации экспертам.

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

В случае кражи информационного источника, следователь должен выяснить отличительные свойства технического средства с целью возможности его дальнейшей идентификации, когда и кем оно использовалось, выяснить,

подключено ли техническое средство к сети, установлено ли на нем программное обеспечение, позволяющее определить его местонахождение, и провести мероприятия для определения его местонахождения.

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.

Если известно, что лицо является специалистом в области информационных технологий и что на его техническом устройстве может храниться компьютерная информация, имеющая значение для расследования преступления, то необходимо более детально изучить его знания, навыки работы с программным обеспечением, где необходимым действием является обязательное привлечение специалиста в аналогичной области. Если по вине лица произошла утечка компьютерной информации, то необходимо выяснить возможные каналы утечки информации.

б) Компьютерная информация содержит специфические сленговые выражения.

В случае, если было установлено, что компьютерная информация находится на тематическом ресурсе, где применяются различные сленговые выражения, актуальным видится привлечение специалиста, разбирающегося в данной теме, а также понимающем значение употребляемых терминов[1].

С учетом изложенного, можно сделать вывод о том, что качество работы следователя и его результативность определяется, в том числе, правильной организацией расследования преступлений. При этом крайне важно не упустить из внимания обстоятельства, определяющие эффективность такого организационного процесса. Уже на подготовительном этапе, а именно до выезда на место

[1] Платёнкин А.В. Особенности использования электронных доказательств при проведении допроса подозреваемого // World science. – 2016. – № 5 (9). – С. 10.

совершения преступления или перед проведением следственных действий, следователь, правильно организовав процесс расследования, может получить определенную компьютерную информацию из банков данных МВД и иных вневедомственных информационных источников, в том числе из различных интернет - ресурсов.

На последующем этапе, например, после выезда на место совершения преступления, компьютерная информация о преступлении может быть получена при выдвижении и проверке нескольких версий, так как интересующие сведения могут присутствовать как на компьютерном устройстве, принадлежащем подозреваемому, так и на устройстве, не принадлежавшем последнему, но при помощи которого мог быть зафиксирован факт совершения преступления или запечатлены причастные к совершению преступления лица. Дальнейший этап организации расследования преступления будет требовать проведения ряда следственных и оперативно-розыскных мероприятий, целью которых будет являться получение необходимой информации с последующим ее процессуальным оформлением.

Получение компьютерной информации на различных этапах расследования должно стать обязательным действием при организации расследования преступления. И исходя из особенностей расследования преступлений, связанных с использованием компьютерной информации, стоит признать, что следователю при возникновении затруднений в процессе изучения всех обстоятельств дела не обойтись без тесного взаимодействия как с сотрудниками оперативно-розыскных подразделений, так и с различными специалистами, которые могут быть привлечены для расследования преступлений в рассматриваемой нами области. В этой связи, при организации расследования преступлений, а также с целью эффективного влияния на установление всех обстоятельств уголовного дела, необходимо более детально рассмотреть механизм взаимодействия следственных и оперативно-розыскных подразделений, а также изучить вопросы привлечении к расследованию специалистов, обладающих определенными (специальными) знаниями в сфере компьютерных технологий.

§ 2.2. Взаимодействие следственных и оперативно-розыскных подразделений при получении компьютерной информации в целях расследования преступлений

Содержание предыдущего параграфа свидетельствует об очевидной актуальности взаимодействия между подразделениями правоохранительных органов в процессе планирования расследования преступлений. Органам правоохранительных систем приходится работать в сложных условиях противодействия расследованию, из-за чего становится очевидным, что одному следователю раскрывать преступления практически не под силу[1].

Следует указать, что результативная борьба с преступностью с использованием компьютерной информации в современных условиях не представляется без тесного взаимодействия на всех этапах расследования именно с оперативными сотрудниками подразделений органов внутренних дел[2].

При раскрытии и расследовании преступлений как следователь, так и оперативный сотрудник должны быть профессионалами своего дела, должным образом выполнять возложенные на них обязанности и процессуальные полномочия для достижения положительного результата. В ранее действующем приказе МВД РФ № 334 «Об утверждении Инструкции по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений» обращалось внимание на то, что «В работе по раскрытию преступлений реально участвует лишь каждый десятый сотрудник, не в полной мере используются криминалистические средства и методы, на низком уровне остается их организация»[3]. Положение дел с тех пор так и не изменилось, сложившуюся ситуацию целесообразно выправлять.

---

[1] Данильян С.А. Взаимодействие органов правоохранительных систем. Монография / С.А. Данильян.- Краснодар: КубГАУ. – 2016. – С.58-59.

[2] Гайдин А.И. Особенности взаимодействия следователя с должностными лицами правоохранительных органов при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Вестник Воронежского института МВД России. – 2020. – №. 3. – С. 177.

[3] Приказ от 20 июня 1996 г. № 334 «Об утверждении инструкции по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений» / Утратил силу в связи с изданием Приказа МВД РФ от 26.03.2008 № 280дсп // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=390400#09107784133705303 (дата обращения:

Практические работники как следственных, так и оперативных подразделений зачастую не имеют достаточно четкого представления о сущности и формах взаимодействия при получении компьютерной информации касательно расследуемого преступления. Взаимодействие следственных и оперативных подразделений в сфере противодействия преступности, где использовалась компьютерная информации, не приобрело системности и подчас носит эпизодический характер. Следователь при проверке версий не всегда эффективно и оперативно может использовать следственные действия, что приводит к невозможности вовремя получать значимую компьютерную информацию и к ее утрате в процессе расследования преступлений. Следственные и оперативные подразделения могут использовать разнящиеся методы сбора и анализа компьютерной информации, что также иногда затрудняет совместную работу.

Однако, если правильно организовать и скоординировать процесс расследования, четко распределить обязанности между следователем и оперативным сотрудником, то это позволит получить не только максимальный объем компьютерной информации, но и затратить меньше усилий в процессе расследования.

Заметим, что нет и более-менее единого подхода к определению понятия «взаимодействие» в юридической науке, что также негативно влияет на его понимание в правоприменительной практике.

Анализируя проблему взаимодействия следственных и оперативно-розыскных подразделений, отметим, что под ним учеными понимается основанная на законе и согласованная деятельность, направленная на раскрытие преступлений и решение поставленных задач[1].

Согласимся с понятием, высказанным учеными, однако добавим, что такая согласованная деятельность возможна при постоянном получении и обмене информацией, имеющей значение для расследования.

27.02.2025).

[1] Яблоков Н.П. Криминалистика. 2-е изд. перераб и доп. М.: Юрайт, 2014. – С. 148.

Это выполнимо лишь в тех случаях, когда следователи и оперативные работники применяют свои профессиональные навыки в проведении совместных мероприятий. Отсутствие взаимодействия или, наоборот, недостаточное разграничение компетенций следователя и оперативного работника наносит существенный вред делу борьбы с преступностью.

Каждая из взаимодействующих сторон должна выполнять свойственные ей обязанности. Только при условии, когда стороны четко представляют свои задачи и не перепоручают их выполнение друг другу, можно говорить об успешной организации расследования преступления. В связи с этим не следует поручать оперативным работникам проведение таких мероприятий и действий, которые следователь может без затруднений выполнить сам. Здесь будет не лишним упомянуть определение Конституционного суда РФ от 27.02.2018 № 328-О, в котором говорится о том, что не допускается подмена следственных действий оперативно-розыскными мероприятиями[1].

В свою очередь, оперативные работники должны прилагать максимум усилий для установления всех возможных источников компьютерной информации, а также для выяснения иных обстоятельств, имеющих отношение к преступлению, где могла бы использоваться компьютерная информация.

По мнению Р.С. Белкина, информация, имеющая отношение к раскрытию и расследованию преступлений, является как доказательственной, так и ориентирующей[2]. Из чего следует, что наиболее эффективного взаимодействия можно достичь в том случае, если оно будет направлено на получение и передачу не только доказательной информации, но и такой, что ориентирует и служит основой для получения и установления фактов, которые имеют отношение к предмету доказывания.

Ориентирующая информация, приобретая в дальнейшем доказательное значение, способствует скорейшему установлению всех обстоятельств дела и, в

[1] Определение Конституционного Суда РФ от 27.02.2018 N 328-О Об отказе в принятии к рассмотрению жалобы гражданина Рачкова Станислава Евгеньевича на нарушение его конституционных прав статьями 6, 7 и 8, пунктом 1 части первой статьи 15 Федерального закона «Об оперативно-розыскной деятельности». – URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-27022018-n-328-o/ (дата обращения 08.02.2025).

[2] Белкин Р.С. Криминалистическая энциклопедия. М.: Издательство Бек, 1997. – С. 84.

конечном счете, ведет к раскрытию преступления.

Следует отметить, что компетенция следственных и оперативных подразделений разная. Следователь, в частности, не может использовать негласные средства и методы получения информации, в свою очередь, оперативному работнику не стоит проводить какие-либо действия без согласования со следователем. Таким образом, следователь и оперативный работник действуют каждый в рамках своей компетенции, используя при этом соответствующие силы, средства и методы.

Вместе с тем, следователю не стоит забывать о поиске и изъятии традиционных следов, которые преступник мог оставить (отпечатки пальцев рук на клавиатуре, системном блоке и других предметах), а также микроследов различного происхождения.

В процессе взаимодействия во время расследования преступлений важным фактором является построение правильной и четкой линии поведения субъектов, задействованных в совместной деятельности.

Так, В.С. Бородин называет обязательные компоненты эффективной совместной деятельности (взаимодействия) во время расследования, а именно:

1) согласованное планирование;

2) распределение обязанностей между субъектами;

3) постановка перед субъектами четких и конкретных задач;

4) своевременный обмен информацией;

5) контроль[1].

Вполне согласны с автором и считаем, что именно такие компоненты совместной деятельности должны лежать в основе взаимодействия следователя с оперативными подразделениями во время расследования преступлений, и, в частности, там, где может быть использована полученная компьютерная информация.

[1] Бородин В.С. Системный подход к организации взаимодействия органов досудебного следствия и дознания // Ученые записки Таврического национального университета имени В.И. Вернадского. Серия: Юридические науки. – 2011. – Т. 24. – № 2 (63). – С. 243-244.

Дальнейшие мероприятия и следственные действия по раскрытию и расследованию определенного факта, связанного с получением компьютерной информации, во многом определяются содержанием информации, полученной в результате проведения оперативных мероприятий.

Обобщение практики свидетельствует о том, что эффективность борьбы с преступной деятельностью, где использовалась компьютерная информация, зависит от оптимального использования всех имеющихся в распоряжении оперативных подразделений сил, средств и методов ОРД. Чтобы эта борьба была целеустремленной, оперативному работнику необходимо владеть оперативной обстановкой, которая бы характеризовала состояние преступности, в том числе и таких преступлений, где использовалась компьютерная информации.

Дальнейшую работу подразделений ОВД необходимо организовать так, чтобы любой сотрудник еще на подготовительном этапе мог получить компьютерную информацию, представляющую интерес, а затем уже с ее учетом 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 путем изучения программного обеспечения, использовавшегося для оплаты, маркетплейсов (Ozon, Wildberries, Яндекс Маркет, AliExpress и др.), а также досок объявлений (Avito, youla);

- выявлять лиц, которые проявляют повышенный интерес к изучению специальной литературы, к примеру, относительно особенностей разработки и использования вредоносного программного обеспечения, выяснить, используют ли они средства шифрования для выхода в сеть Интернет. Здесь стоит указать, что у правоохранительных органов должна быть база интернет-сайтов, где возможно приобретение вредоносного программного обеспечения или где описаны механизмы обхода компьютерной защиты;

- установить путем использования различных поисковых интернет-сервисов, пытался ли пользователь приобрести или сбыть запрещенные к обороту товары и т. п.

Кроме того, весьма полезную компьютерную информацию в ходе расследования преступления оперативный работник может получить:

- от разработчиков программного обеспечения;

- от лиц, занимающихся монтажом и настройкой оборудования;

- от пользователей тематических форумов;

- от операторов связи и организаций, предоставляющих интернет-услуги.

Следователь же, с учетом информации, полученной из названных источников, в дальнейшем получает компьютерную информацию, представляющую интерес, о расследуемом факте путем осуществления следственных действий – осмотров, обысков, назначения криминалистических экспертиз и тому подобное.

Кроме того, при производстве ряда следственных действий, например, допросе, параллельно с его проведением оперативный работник может получить информацию о данном лице из банков данных МВД для установления наличия судимости и за какие преступления, а также получить объективную информацию о личности задержанного из других гласных и негласных источников. Следовательно, только при наличии такого взаимодействия следователя и оперативного работника можно говорить о получении полной, достоверной, объективной информации об определенном факте действий, связанных с использованием компьютерной информации.

Как уже отмечалось, особенностью расследования преступлений, связанных с получением компьютерной информации, является то, что первоочередное значение при получении доказательств имеет оперативная информация, поскольку она обеспечивает установление обстоятельств совершенного преступления.

Поскольку следователь и оперативный работник решают общую задачу по установлению и разоблачению преступника, то оба заинтересованы в том, чтобы наиболее полно использовать все возможные средства для раскрытия

преступления. Поэтому ознакомление следователя не только с компьютерной информацией, но и со способом ее получения будет способствовать более эффективному ее применению. Это, в свою очередь, поможет следователю выбрать самые целесообразные тактические приемы по ее реализации.

Конечно, могут возникнуть возражения относительно целесообразности ознакомления следователя с материалами, полученными в процессе применения оперативно-розыскных мероприятий. Применимо к компьютерной информации с таким возражением трудно согласиться. Как отмечает С.В. Коровин, возможность следователя знакомиться с оперативно-розыскными материалами запрещена. Вместе с тем, не зная способов и источников получения оперативной информации, следователь иногда затрудняется дать оценку ее достоверности[1]. Бесспорно, только правильное сочетание следственных действий с оперативно-розыскными мероприятиями при строгом соблюдении законности позволит успешно решить задачи быстрого и полного раскрытия преступлений.

Таким образом, знание следователем основ оперативной работы необходимо совсем не для того, чтобы вмешиваться в деятельность сотрудников оперативных аппаратов, а для того, чтобы знать возможности оперативно-розыскных мероприятий, чтобы взаимодействие следователя и оперативного работника было глубоко осознанным обеими сторонами.

Особое место в процессе взаимодействия отводится и его формам. Исчерпывающий перечень форм взаимодействия приводит А.П. Кругликова. Мы не будем перечислять их все, а лишь отметим те, которые наиболее подходят к вопросу получения компьютерной информации в процессе расследования преступлений, это такие как:

1) совместное планирование по делу следственных действий, розыскных и оперативно-розыскных мероприятий;

2) выполнение органом дознания следственных действий по поручениям следователя;

[1] Коровин С.В. Взаимодействие сотрудников оперативных аппаратов и органов предварительного следствия в расследовании и раскрытии бандитизма (методические рекомендации). – Тюмень. – 2007. – С. 9.

3) выполнение органом дознания, оперативными подразделениями, оперативно-розыскных мероприятий по поручениям следователя;

4) содействие органа дознания следователю при производстве отдельных следственных действий;

5) обмен информацией и совместное обсуждение результатов следственных действий и оперативно-розыскных мероприятий, произведенных в процессе взаимодействия;

6) участие должностных лиц органов дознания, оперативных органов, осуществляющих оперативно-розыскную деятельность, в деятельности следственных групп[1].

Выделим основные направления предложенных форм с учетом поиска и использования компьютерной информации в расследовании преступлений.

Форма планирования заключается в составлении совместных планов следственных действий и оперативно-розыскных мероприятий с учетом общего плана расследования. По сути, планы предусматривают комплексное вовлечение в процесс расследования различных сил и средств, что предполагает обеспечение координации деятельности участников расследования, постоянный обмен информацией и компьютерной информацией, иначе говоря, реальное взаимодействие. Наряду с этим, для выполнения отдельных пунктов общего плана и учитывая специфику задач, решаемых конкретным подразделением, следователь может давать поручения согласно ч. 3 ст. 7 ФЗ «Об оперативно-розыскной деятельность», где сказано, что основания для осуществления ОРМ «могут содержаться в поручениях следователя, руководителя следственного органа, … по уголовным делам и материалам проверки сообщений о преступлении, находящимся в их производстве».

В п. 2 ст. 14 этого Закона указывается, что подразделения, которые осуществляют ОРД, обязаны «исполнять в пределах своих полномочий поручения в письменной форме дознавателя, органа дознания, следователя, руководителя

[1] Кругликов А.П. О понятии и системе форм взаимодействия следователей и органов дознания в процессе расследования и раскрытия преступлений // Успехи современной науки. – 2017. – № 3. – С. 193.

следственного органа о проведении оперативно-розыскных мероприятий по уголовным делам и материалам проверки сообщений о преступлении, принятым ими к производству, а также решения суда по уголовным делам.»

Становится очевидным, что для обеспечения координации во время планирования взаимодействия обязательным является обмен информацией.

Особенно хотим обратить внимание на то, что обязательным компонентом в этой структуре выступает компьютерная информация, которая влияет и на процесс составления плана, и на эффективность взаимодействия в целом.

Итак, основными условиями, которые влияют на планирование расследования преступлений, связанных с получением компьютерной информацией, являются: наличие у следователя исходной информации относительно преступления; четкая и реальная оценка сложившейся следственной ситуации; объективный учет возможностей решения задач расследования; оценка обстоятельств и времени, которое отводится для решения поставленных задач.

Стоит отметить, что деятельность следователя исключает сочетание процессуальных и оперативно-розыскных функций. Следователь не должен вмешиваться в оперативно-розыскную деятельность, а оперативный работник – посягать на процессуальную самостоятельность следователя. Работники оперативно-розыскных подразделений и следователь выполняют каждый свои функции и сами выбирают, какие мероприятия им проводить, но успех их деятельности зависит от ее согласованности.

Поэтому следователь в поручении не должен устанавливать, какое ОРМ необходимо проводить оперативным подразделениям, однако он может конкретизировать определенные направления поиска компьютерной информации, имеющей значение в процессе расследования. Следователь может выразить поручение словами «осуществить оперативно-розыскные мероприятия с целью установления лиц, располагающих компьютерной информацией о совершенном преступлении» или «осуществить оперативно-розыскные мероприятия с целью установления источников компьютерной информации».

Также следователь может дать и более конкретные поручения «с целью получения компьютерной информации о контакте подозреваемого с другими лицами в какой-то промежуток времени», «с целью розыска предметов в сети Интернет, которые могут принадлежать подозреваемому». Могут быть и другие вопросы, которые в интересах уголовного производства должны проверяться путем осуществления оперативно-розыскной деятельности.

Что касается обмена информацией, то здесь необходимо предостеречь следователей от взаимодействия с отдельными работниками подразделений, осуществляющих оперативно-розыскную деятельность, которые могут утверждать, что они имеют достоверные сведения о преступной деятельности лица, не обращая внимания на факт, что они не оформлены должным образом. С целью приобретения компьютерной информации доказательственного значения ее необходимо обличить в процессуальную форму, зафиксировав ее письменно.

Общеизвестно, что вся деятельность правоохранительных органов основывается на нормах закона, которыми необходимо руководствоваться, поэтому и оперативные работники во время проведения ОРД и получения компьютерной информации должны опираться на действующую законодательную базу, чтобы не нарушить общеобязательных правил и не превысить пределов дозволенного. На данном этапе возникают вопросы правового регулирования передачи компьютерной информации. Законодатель, ограничившись «Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд», не указывает четкие рамки представления цифровых доказательств, что может привести к сложностям в дальнейшем процессе обмена компьютерной информацией между оперативным сотрудником и следователем.

Основным условием быстрого и качественного раскрытия и расследования преступлений одновременно в нескольких направлениях, в разных местах с параллельной отработкой всех следственных версий в уголовном производстве, а также возможности сосредоточивать усилия на одном важном этапе – является взаимодействие в расследовании преступлений через создание следственно-

оперативных групп (далее – СОГ). Как свидетельствует практика последних лет, опыт расследования преступлений при помощи СОГ достаточно обогатился. Кроме того, при создании СОГ привлекаются наиболее опытные работники всех подразделений в зависимости от уголовной характеристики преступления. Создание групп в сложных уголовных производствах и со значительным объемом работы предоставляет ряд преимуществ относительно других форм взаимодействия следствия с оперативными сотрудниками. По мнению С.Н. Юсупкадиева, СОГ является одним из самых эффективных видов взаимодействия для расследования тяжких преступлений. Ученый считает, что основными факторами, которыми обусловлена необходимость процессуального взаимодействия следователя с оперативными подразделениями в составе СОГ, являются следующие:

1. Следственные действия и оперативно-розыскные мероприятия членов группы имеют одинаковую цель, направленную на быстрое раскрытие и расследование преступлений.

2. Все действия участников СОГ координируются и согласуются между собой во время разработки единого плана.

3. Каждый из участников СОГ действует в пределах своих полномочий и сохраняет свою функциональную самостоятельность.

4. Работа в составе СОГ дает следователю возможность быстрее использовать полученные оперативным путем данные, а оперативным сотрудникам – информацию, полученную во время проведения следственных действий[1].

Также создание СОГ повышает ответственность того или иного сотрудника как следствия, так и оперативного подразделения, отвечающего за определенный пункт порученной работы по конкретной версии, выдвигаемой при раскрытии и расследовании уголовного правонарушения.

[1] Юсупкадиева С.Н. Этапы и формы взаимодействия следователя с другими службами ОВД при раскрытии и расследовании преступлений // Фундаментальные и прикладные исследования: проблемы и результаты. – 2014. – № 10. – С. 265.

Сказанное позволяет сделать вывод о том, что к расследованию преступлений, где могла быть использована или получена компьютерная информация о нем, необходимым является комплексный подход, то есть умелое сочетание следственной и оперативной работы, согласованной, взаимодополняющей друг друга, подчиненной единой цели.

Получение компьютерной информации в расследовании актуализирует необходимость теснейшего делового взаимодействия между следователем и оперативными сотрудниками. Такое взаимодействие позволяет:

- начиная со стадии проверки информации относительно совершенного преступления, в полной мере использовать все возможности научно-технических средств;

- на основании компьютерной информации, полученной оперативным путем, тщательно разрабатывать и выдвигать следственные версии, делать правильный выбор тактических приемов и определять наиболее эффективную последовательность производства следственных действий и некоторых оперативно-розыскных мероприятий.

На наш взгляд, наиболее эффективными формами взаимодействия при использовании компьютерной информации в расследовании могут являться:

- совместное планирование, обеспечивающее организованность и согласованность всех действий в процессе расследования преступлений, с целью избежать дублирования действий и обеспечить максимальную эффективность расследования;

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

- совместные 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;

- взаимообмен информацией в целях качественной организации и проведения ОРМ, следственных действий с должностными лица экспертных подразделений органов внутренних дел и сотрудниками иных подразделений (центра информационных технологий, связи и защиты информации (ЦИТС и ЗИ) ГУ МВД России по субъектам РФ, главного информационно-аналитического центра (ГИАЦ) и др.), являющихся носителями специальных знаний в сфере компьютерной техники и информационных технологий[1];

- привлечение специалистов в области компьютерных технологий к расследованию преступлений.

Однако эффективность взаимодействия требует от лиц, занимающихся расследованием преступлений, принятия своевременных оптимальных решений для скорейшего установления всех источников, где могла сохраниться компьютерная информация. Успешное решение задач расследования возможно лишь при условии тесного взаимодействия следственных и оперативных подразделений не только во время совместного планирования следственных действий, оперативно-розыскных мероприятий, действий экспертно-криминалистических подразделений но и при их выборе, разработке и использовании тактических приемов, изъятии и сохранении вещественных доказательств с использованием технических средств, оптимизации законодательной базы и внедрении современных информационных технологий для облегчения анализа и передачи информации, что мы непременно в дальнейшем рассмотрим в нашей диссертации.

[1] Гайдин А. И. Особенности взаимодействия следователя с должностными лицами правоохранительных органов при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Вестник Воронежского института МВД России. – 2020. – №. 3. – 181.

§ 2.3. Получение компьютерной информации посредством использования специальных знаний

Использование специальных знаний в раскрытии и расследовании преступлений является важной составной частью борьбы с отдельными видами преступлений, к которым относятся и те, что совершаются при помощи компьютерной информации. Развитие современных возможностей получения, хранения и передачи компьютерной информации указывает на необходимость использования специальных знаний при обнаружении и фиксации компьютерной информации и требует комплексного подхода, охватывающего как технические, так и юридические аспекты.

Стоит признать, что сотрудники ОВД, непосредственно осуществляющие борьбу с преступностью в сфере информационных технологий, слабо подготовлены профессионально для осуществления достаточно трудоемких и сложных мероприятий по поиску компьютерной информации, имеющей значение в расследовании преступлений.

Это подтверждается как статистикой, так и тем, что поиск значимой в расследовании компьютерной информации при помощи компьютерных технологий подчас носит хаотичный характер. Исследование, проведенное В.И. Шаровым, показало, что чаще всего способы поиска значимой в расследовании информации сотрудниками полиции осуществляются путем ее запроса в: поисковых системах (35%), социальных сетях (27%), блогах, чатах (6%), сайтах фирм, организаций и предприятий (19%), сайтах СМИ (11,5%).

В ходе исследования были заданы еще два вопроса, связанные с необходимостью использования способов, позволяющих получать и копировать информацию с закрытых паролями аккаунтов. На необходимость просмотра электронной почты указали 28% респондентов, аккаунтов в социальной сети – 38% опрошенных лиц, аккаунтов в иных сервисах (gmail, mail.ru, игровых аккаунтов, аккаунтов журналов, электронных магазинов, личных кабинетов в электронном банкинге, в том числе с привязанными к ним счетами или платежными картами) –

34% респондентов. Однако реально проводили данные действия соответственно 18%, 55%, 27% опрошенных[1].

Важным шагом для эффективного раскрытия и расследования преступлений, совершаемых при помощи компьютерной информации, является привлечение специалиста. Также стоит отметить, что раскрытие киберпреступлений иногда невозможно и без использования современных информационных технологий, в том числе технологий искусственного интеллекта, где также необходимо обладать специальными знаниями и навыками.

Ранее проведенный нами анализ законодательства, связанный с получением компьютерной информации, показывает, что в РФ правовая регламентация в этом направлении не успевает за развитием информационных технологий. Не изучены и тем более не разработаны четкие пути и способы, методики и механизмы в целом, связанные с практической реализацией норм закона, которые регулируют возможность доступа к зашифрованной компьютерной информации при расследовании и раскрытии преступлений. Отсутствуют нормативные акты, которые регулировали бы внедрение искусственного интеллекта в правоохранительную деятельность.

Бесспорно, преступления, совершаемые при помощи компьютерной информации, не остаются без внимания ОВД. Так, существенный вклад в борьбу с киберпреступностью обеспечивает Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий[2]. В Следственном комитете при МВД России также создан отдел по организации расследования преступлений в сфере компьютерной информации, а в следственных управлениях крупных регионов – специализированные подразделения по расследованию данного вида преступлений[3]. Однако их деятельность направлена, в основном, против преступлений, закрепленных в главе

[1] Шаров В.И. Интернет как источник оперативно-розыскной и процессуальной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 3(35). – С. 113.

[2] Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий [Электронный ресурс]. – URL: https://мвд.рф/mvd/structure1/Upravlenija/убк (дата обращения: 27.02.2025).

[3] Воронов И.А. Зарубежный опыт борьбы с киберпреступностью [Электронный ресурс]. – URL: http://www.crime-research.ru (дата обращения: 19.01.2025).

28 УК РФ. При этом соответствующие подразделения руководствуются исключительно установленными и утвержденными законодательными актами, которые отстают от развивающихся технологий, что исключает оперативность реагирования на возникающие обстоятельства и, что самое главное, на предотвращение событий до их наступления.

Не смотря на отсутствие нормативных актов, регулирующих шифрование компьютерной информации и деанонимизацию, практики не оставляют без внимания это направление. Теоретически перехватывать и расшифровывать трафик пользователей можно уже сейчас, уверен аналитик центра мониторинга и противодействия киберугрозам Solar JSOC Алексей Павлов. Речь идет о так называемой атаке «человека посередине». Пользователь направляет трафик на свой почтовый сервер, но провайдер пропускает его через собственный сервер, где трафик может благополучно расшифровываться, сохраняться и зашифровываться для передачи дальше, объясняет А. Павлов[1].

На открытых ресурсах сети Интернет можно встретить массу рекомендаций по расшифровке трафика, например, при помощи того же метода «человек посередине», однако реализовать данную атаку и схожие с ней без специальных знаний в области программирования видится весьма затруднительным. Стоит учитывать и то, что в настоящее время разработчики программного обеспечения самостоятельно осуществляют шифрование передаваемой компьютерной информации и свободны в выборе способов шифрования, что дает преимущества злоумышленникам, имеющим знания в этой области, в отличие от сотрудника ОВД, которому еще необходимо разбираться в неизвестной ему сфере.

Немаловажным является то, что одна из основных трудностей борьбы с преступлениями в сфере компьютерной информации, в первую очередь, связана с доступностью самого орудия преступления на различных ресурсах сети Интернет. Так, при помощи поисковых систем в открытом доступе можно найти бесчисленное множество пособий и видеоуроков, направленных на обучение

[1] К Яровой нет ключа [Электронный ресурс]. – URL: http://www.vedomosti.ru/newspaper/articles/2017/02/16/678086-yarovoi-klyucha (дата обращения: 07.02.2025).

совершению противоправных действий. В Интернете существуют и сайты, где можно скачать программы, целью которых является поиск уязвимости в программном обеспечении или при помощи которых осуществляется проведение атаки на вычислительную систему. Если изучить методы и способы, используемые злоумышленниками, и применив их, сотрудники ОВД могут самостоятельно получать значимую в расследовании преступлений компьютерную информацию.

В своей деятельности киберпреступники используют определенные алгоритмы действий и способы совершения преступлений, которые нужно учитывать сотрудникам правоохранительных органов при поиске компьютерной информации. Такая деятельность была наиболее успешно систематизирована в модели The Cyber Kill Chain (разработанной компанией Lockheed Martin).

Согласно этой модели, успешная атака на информационную инфраструктуру организации состоит из семи фаз:

1. Разведка (reconnaissance), то есть сбор общедоступной информации об объекте атаки.

2. Подготовка инструментария (weaponization), прежде всего – вредоносного ПО, с учётом особенностей инфраструктуры объекта атаки.

3. Доставка (delivery) вредоносного ПО на атакуемый объект.

4. Внедрение вредоносного ПО с использованием уязвимостей (exploitation).

5. Использование внедренного вредоносного ПО для развёртывания дополнительных инструментальных средств (installation), необходимых для развития атаки.

6. Использование внедренных инструментальных средств для удалённого доступа к инфраструктуре и получения контроля над ней (command and control).

7. Достижение целей нарушителя (actions on objective)[1].

Так, например, чтобы скрыть свои следы, хакер может изменить mac-адрес, IP-адрес, получить доступ к сети Интернет из неконтролируемой сети (места с бесплатным Wi-Fi), использовать proxy-сервер или удаленный (захваченный)

[1] Моделирование угроз на основе сценариев или Как Cyber Kill Chain и ATT&CK помогают анализировать угрозы ИБ URL: https://safe-surf.ru/specialists/article/5247/626649/ (дата обращения:13.02.2025).

компьютер как шлюз.

Получение доступа к компьютерной системе удаленного компьютера возможно благодаря взлому пароля или использованию эксплойтов.

Эксплойты – это подвид вредоносных программ. Они содержат исполняемый код, направленный на использование уязвимостей в программном обеспечении и применяемый для проведения атаки на вычислительную систему на локальном или удаленном компьютере[1].

В лаборатории Касперского указывают, что есть два способа «скормить» пользователям эксплойты. Во-первых, при посещении ими сайта, содержащего вредоносный код эксплойта. Во-вторых, при открытии пользователем безобидного на вид файла со скрытым вредоносным кодом. Как легко догадаться, во втором случае для доставки эксплойта, как правило, пользуются спамом или фишинговым письмом. Использование уязвимостей в легитимном программном обеспечении для атак на компьютеры пользователей – одна из самых острых проблем индустрии информационной безопасности. Уязвимости позволяют заражать компьютер вредоносным программным обеспечением незаметно для пользователя, а зачастую – и для защитного решения, установленного на компьютере.

В этом и заключается основная привлекательность эксплойтов для киберпреступников – в отличие от других способов заражения компьютера, большинство из которых основаны на социальной инженерии и далеко не всегда оказываются эффективными, метод заражения через уязвимости пока еще способен дать злоумышленникам возможность достичь цели[2]. Обычно эксплойты являются платными, цены на них колеблются от 100[3] до 1800 долларов[4]. Однако существуют и такие эксплойты, доступ к которым можно получить бесплатно.

Еще одним способом получения компьютерной информации является поиск

---

[1] Что такое эксплойты и почему их все так боятся? [Электронный ресурс]. – URL: https://blog.kaspersky.ru/exploits-problem-explanation/8459/ (дата обращения: 09.02.2025).

[2] Введение: почему мы решили анализировать Java. [Электронный ресурс]. – URL: https://securelist.ru/analysis/obzor/20794/otchet-laboratorii-kasperskogo-java-pod-udarom-evolyuciya-eksplojtov-v-2012-2013-gg/ (дата обращения: 22.02.2025).

[3] Большой обзор свежих эксплойт-пакетов. [Электронный ресурс]. – URL: https://xakep.ru/2015/04/09/195-exploit-packs/ (дата обращения: 22.02.2025).

[4] Эксплойт-пак для новичков. [Электронный ресурс]. – URL: http://www.truehackers.ru/articles/vulnerabilities/4394-jeksplojtpak-dlja-novichkov (дата обращения: 28.01.2025).

уязвимостей и взлом путем SQL-инъекций, SSRF-атаки (Server-Side-Request-Forgery) и RCE-уязвимости (Remote Code Execution).

SQL-инъекция позволяет получить доступ к базе данных сайта или сервиса, в которых могут храниться логины, пароли и прочие сведения о пользователях, включая данные администратора.

С помощью SSRF-атаки потенциальный злоумышленник может обращаться ко внутренней инфраструктуре компании, иногда недоступной даже из Глобальной сети.

RCE – уязвимость, позволяет преступнику получить полный административный доступ к компьютеру и выполнять команды от его имени.

Иногда и очень опытные специалисты пропускают или попросту не успевают закрыть уязвимости в системе безопасности. Например, против zero day – уязвимостей далеко не все могут бороться.

На самом деле поиск уязвимостей не всегда является трудоемкой задачей для специалиста в области информационных технологий. Кроме изучения инфраструктуры сети, киберпреступник может воспользоваться открытыми для всеобщего пользования сервисами Shodan и Censys[1]. При помощи таких сервисов возможно получить список устройств, имеющих уязвимости и не защищенных от какой-то конкретной известной угрозы.

После получения доступа к компьютеру, преступник может поместить на нем вредоносное программное обеспечение (троянскую программу) для перехвата информации или получить доступ к базе данных сайта, где хранятся логины, пароли, а также личная информация пользователей.

Таким образом, вышеизложенное подтверждает тот факт, что, в настоящее время сложилась благоприятная ситуация для использования технических средств в подготовке, совершении, сокрытии преступлений и оказании противодействия правоохранительным органам в раскрытии и расследовании противоправной

[1] Чем занимается «белый хакер», как им стать и сколько можно заработать [Электронный ресурс]. – URL: https://vc.ru/story/86714-chem-zanimaetsya-belyy-haker-kak-im-stat-i-skolko-mozhno-zarabotat?from=digest&date=081019 (дата обращения: 12.01.2025).

деятельности[1].

Это в значительной степени обусловлено также тем, что не существует сколько-нибудь конкретных и полных по содержанию методологических разработок по организации применения специальных знаний в процессе расследования и предупреждения преступлений рассматриваемой категории.

А.Ю. Маруев приходит к выводам, что повышение качества информационной работы во многом зависит от умелого внедрения новейших аналитических методов и технологий, использования всей совокупности наличных информационных источников. Постоянное внимание следует уделять использованию передовых методик и способов получения информации, обмену опытом в этой области, а также подготовке квалифицированных кадров в области работы с информацией на основе высших профессиональных стандартов[2].

Зачастую ученые при освещении вопросов, связанных с получением компьютерной информации, акцентируют внимание на проблемах, связанных с отсутствием специальных знаний в области использования компьютерных технологий, а также дорогостоящего оборудования и высокоскоростных каналов связи. В связи с этим, несмотря на огромные возможности современных средств обеспечения розыскных мероприятий и следственных действий, далеко не всякая информация может быть оперативно получена и зафиксирована без участия специалиста.

Лантух Э.В., Ишигеев В.С., Грибунов О.П. убеждены, что именно своевременное привлечение специалиста может существенно облегчить работу следователя. При производстве следственных действий в качестве специалистов в сфере информационных технологий могут привлекаться как сотрудники различных организаций, обладающие профессиональными знаниями работы с компьютерной техникой и информационными технологиями при наличии у них

---

[1] Шурухнов Н.Г. Современная преступность (истоки, направленность, техническая оснащенность, способы совершения, сокрытия): содержание рекомендаций по раскрытию и расследованию // Известия ТулГУ. Экономические и юридические науки. – 2013. – № 4-2. – С. 134.

[2] Маруев А.Ю. Информационная безопасность России и основы организации информационного противоборства // Проблемный анализ и государственно-управленческое проектирование. – 2010. – № 1. – С. 54.

диплома об образовании в области информационных технологий, так и эксперты экспертно-криминалистических центров МВД России[1].

Однако, взаимодействие следователя и эксперта-криминалиста более ограничено по времени и проявляется в основном тогда, когда требуются специальные знания в области работы со специальным программным обеспечением, а также для криминалистического исследования вещественных доказательств с целью обнаружения, фиксации и изъятия следов преступного поведения лиц, осуществляющих незаконные действия с компьютерной информацией. Взаимодействие начинается уже непосредственно на стадии проверки информации о преступлении, в основном сразу же во время проведения осмотра места происшествия.

Осматривая место происшествия, целесообразно иметь предварительную информацию, например, полученную от свидетелей, в том числе о способе использования компьютерной информации и с учетом этого пытаться обнаружить соответствующие следы преступления. При этом не всегда стоит полагаться только на специалиста-криминалиста, участвующего в следственном осмотре места происшествия и предметов. Особенно ценным является участие такого специалиста в осмотре компьютерной техники, хранимой на ней информации, при работе с которой могут потребоваться знания специальных терминов, сленгов, языков программирования и т. д. Еще до проведения экспертизы специалист во время осмотра может обратить внимание следователя на характерные индивидуальные признаки, свидетельствующие о конкретном месте нахождения компьютерной информации, а также отметить, какое программное обеспечение и какие ресурсы мог использовать подозреваемый. Специалист в сфере информационных технологий окажет квалифицированную помощь в выявлении, фиксации и получении компьютерной информации, имеющей важное доказательное значение.

[1] Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Russian journal of criminology. – 2020. –Т. 14. – № 6. – С. 885.

Участие специалиста также бывает необходимо при осмотре технических средств и оборудования, которое могло быть использовано для создания вредоносного программного обеспечения. Так, например, при осмотре места происшествия в случае обнаружения вредоносных программ, изготовленных с помощью определенной компьютерной техники, следует учитывать тот факт, что информация, которая содержится в компьютере, может быть уничтожена или зашифрована, поэтому следует принять меры к ее сохранению, а иногда и восстановлению поврежденных файлов с использованием специальных программ.

Проводя обыски или осмотры в местах нахождения компьютеров и совмещенной с ними техники, следователь должен соблюдать определенные меры безопасности (не выключать работающий компьютер, не извлекать периферийные устройства и т. п.), невыполнение которых может привести к уничтожению вещественных доказательств или существенному их повреждению. Это лишний раз говорит о пользе привлечения к участию в этих действиях специалистов.

Становится очевидным, что для оперативного получения компьютерной информации по выявлению преступления и лица, его совершившего, необходимы навыки и умения, а еще точнее, специализация в области программирования и компьютерных технологий с пониманием способов хранения, передачи информации и возможностей ее расшифровки.

Однако на практике ситуация с привлечением специалиста несколько иная. На вопрос к сотрудникам ОВД привлекали ли они специалиста в области информационных технологий при расследовании преступлений, совершаемых в сфере компьютерной информации, был ответ, что последний в 98 процентов случаев не привлекался[1]. Это связано с тем, что далеко не всегда преступления в сфере компьютерной информации совершаются с использованием вредоносных программ специалистами в области информационных технологий. В большинстве случаев противоправная деятельность реализуется с помощью обычной компьютерной техники, на которую устанавливается стандартное и доступное для большинства пользователей программное обеспечение, т. е. компьютер выступает

[1] См.: Приложение № 1. Опросный лист.

как вспомогательное устройство, при помощи которого совершается преступление. В таком случае участие специалиста может быть не обязательным, а для получения компьютерной информации стоит рассмотреть способы, используемые как сотрудниками ОВД, так злоумышленниками.

Выявленные практические сложности в привлечении специалистов позволяют заключить, что целесообразным является пересмотр подходов к обязательному формальному привлечению специалиста для выполнения всех задач, связанных с компьютерной информацией. Стоит рассмотреть частичную автоматизацию рутинных функций специалиста посредством внедрения систем искусственного интеллекта, способных проводить первичный сбор, анализ и фиксацию компьютерных данных по заданным алгоритмам. Такие системы демонстрируют высокую эффективность, например, в анализе огромных объёмов текстовых материалов для быстрого поиска слов и фраз, которые могут иметь отношение к уголовному расследованию, даже если содержание сообщений было завуалировано или использовались сленговые и разговорные выражения, которые труднее обнаружить. Практика показывает, что ИИ способен выявлять такие скрытые сообщения в 21 раз быстрее человека.[1]

Такой подход позволит следователю или оперативному сотруднику, обладающему базовыми компетенциями, самостоятельно выполнять первоначальные действия по получению и фиксации компьютерной информации. Это значительно ускорит процесс расследования и позволит оперативно реагировать на меняющуюся обстановку.

Однако, это не исключает необходимости привлечения специалиста (или назначения судебной экспертизы) для выполнения сложных, неавтоматизируемых задач, глубокого анализа данных, а также для процессуального оформления и придания доказательствам юридической силы. Роль специалиста в таких случаях становится контролирующей и экспертной, обеспечивая надлежащую фиксацию и

[1] AI can detect abusive messages 21 times faster than humans - Forensic Capability Network. [Электронный ресурс]. – URL: https://www.fcn.police.uk/news/2024-07/ai-can-detect-abusive-messages-21-times-faster-humans (дата обращения: 13.02.2025).

оценку данных, полученных в том числе с помощью ИИ. Таким образом, под «целесообразностью расследования без привлечения специалиста» подразумевается не полный отказ от использования специальных знаний, а оптимизация процесса за счёт автоматизации части функций и повышения уровня подготовки сотрудников ОВД, что позволяет снизить частоту формального привлечения сторонних специалистов для выполнения стандартизированных процедур, при сохранении возможности и необходимости их участия в процессуально значимых и сложных случаях.

Чаще всего действенным и активно применяемым сотрудниками полиции способом поиска и получения компьютерной информации является запрос с ключевыми словами или фразами в поисковых ресурсах сети Интернет или социальных сетях.

Так, с учетом судебной практики[1], нами были выделены следующие способы получения компьютерной информации сотрудниками ОВД:

1) мониторинг и фиксация компьютерной информации в социальных сетях, досках объявлений, специализированных (созданных для осуществления противоправной деятельности) сайтах;

2) физический осмотр содержимого различных компьютерных устройств, в первую очередь, мобильных телефонов, где информация была обнаружена в папке «Галерея» (видео и фотографии), в папке «Диктофон» (аудиозаписи);

3) получение от пользователя логина и пароля к программному обеспечению (мессенджерам «WhatsApp», «Telegram» и др.), используемому для осуществления противоправной деятельности[2].

Начнем с тех источников, доступ к которым не закрыт (открытых источников). В указанном случае, в ходе мониторинга сети Интернет, сотрудники полиции получают информацию из социальных сетей («ВКонтакте», «Одноклассники»), из досок объявлений (https://youla.ru), интернет-магазинов, а также других интернет-

[1] См.: Приложение № 2. Результаты анализа судебных решений.

[2] Павлюков В.В. Практические способы получения и использования результатов оперативно-розыскного мероприятия «Получение компьютерной информации» // Вестник Костромского государственного университета. - 2020. – Т. 26. – № 3. – С. 200.

ресурсов[1].

Способ получения компьютерной информации путем мониторинга сети Интернет наглядно описан в решении Абинского районного суда (Краснодарский край) № 12-40/2018 от 25 мая 2018 г. по делу № 12-40/2018. В материалах дела отмечалось, что в сети Интернет, в поисковике с заданным вопросом: «…» отображены результаты поиска. В ходе анализа предъявленных результатов также установлен сайт объявлений, при осмотре которого выявлено текстовое объявление с информацией об осуществлении миссионерской деятельности. Кроме того, в процессе осмотра доски объявлений установлено, что вышеуказанный сайт находится в открытом доступе, предназначен для публичного просмотра. На странице отображены различные фотографии, свидетельствующие о противоправной деятельности[2].

Стоит отметить, что для получения более информативных в процессе расследования сведений, необходимо проводить поиск на интернет-ресурсах, требующих регистрации пользователей. А.М. Ишин предполагает, что постоянное изучение сообщений, публикуемых в соответствующих чатах, конференциях, на форумах, обеспечивает возможность получения сведений о намерениях участников устанавливать их связи между собой, узнавать детали замышляемых деяний, выявлять признанных лидеров, следить за их перемещениями, вести подбор лиц для привлечения к сотрудничеству и т. д.[3].

Можно предположить, что здесь следователю помогут в большей степени именно его знания, которые он применяет при расследовании преступлений, а не специалиста в области информационных технологий. Так, исследуя компьютерную технику, следователь без углубленных знаний программирования может самостоятельно установить и зафиксировать, на какие интернет-сайты заходил разрабатываемый, где получил противоправную информацию, с какими лицами

---

[1] См.: Приложение № 2. Результаты анализа судебных решений.

[2] Решение Абинского районного суда (Краснодарский край) № 12-40/2018 от 25 мая 2018 г. по делу № 12-40/2018 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/6YL6sesUHsHt/ (дата обращения: 12.02.2025).

[3] Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. – С. 120-122.

вел интернет-переписку, какими интернет-источниками пользовался[1] и т. д. Заметим, что при проведении поиска необходимо акцентировать внимание на наличие в тексте ключевых слов, фраз, в том числе «сленговых» выражений, употребляемых с целью завуалировать содержание сообщений. Анализ полученной в ходе мониторинга информации позволяет установить характер взаимоотношений между фигурантами общения, распределение ролей, технические нюансы при передаче информации.

Существуют различные ситуации, когда передача компьютерной информации осуществляется с помощью различных проприетарных программных продуктов, в том числе с использованием сервисов с надежными средствами шифрования.

Например, до настоящего времени остается не решенным вопрос по тактике получения компьютерной информации из мессенджеров «WhatsApp», «Telegram», «Viber» и т. д. Последние активно используются злоумышленниками для передачи противоправной информации посредством как стационарных компьютеров, так и мобильных телефонов.

Поэтому, для задействования всего потенциала сферы информационных технологий в борьбе с преступностью помимо обычных поисковых запросов в сети Интернет, нужны более действенные способы.

Полагаем, что в целях оперативного выявления неустановленных лиц, совершающих преступления посредством сети Интернет, целесообразно задействовать отдельные способы, которые используют в своей деятельности сами киберпреступники для получения интересующих их данных о пользователе. Помимо рассмотренных ранее эксплойтов злоумышленник, совершая свою противоправную деятельность для получения логинов и паролей на сайтах, все чаще прибегает к созданию и использованию фишинговых сайтов[2].

Взяв на вооружение такой способ при получении компьютерной информации и, воспользовавшись опытом мошенников, оперативный сотрудник может создать

---

[1] Оперативное получение компьютерной информации // Жизнь в законе, портал для ликвидации юридической безграмотности [Электронный ресурс]. – URL: http://lifeinlaw.ru/bez-rubriki/orm.php (дата обращения: 22.02.2025).

[2] Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

и использовать свой сайт для установления данных о киберпреступнике при помощи сети Интернет, строго соблюдая при этом нормы действующего законодательства и принцип отсутствия провокации. Законодатель не запрещает создавать сайты сотрудникам ОВД, более того ст. 11 ФЗ «О полиции» установлено, что полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

Процесс создания сайта не является дорогостоящим, не требует дополнительного специального санкционированного разрешения и не требует знаний программирования. Так, для создания сайта необходимо приобрести домен, создать сайт при помощи специальных сервисов или программ (WordPress, Joomla) и разместить его на хостинге. Уже сейчас все это обойдётся в считанные копейки: по состоянию на 10.02.2025 г. покупка домена в зоне «.ru» на официальном регистраторе доменных имён REG.RU составляет 119 рублей, а месячная стоимость услуг хостинга на этом сайте составляет 229 рублей[1]. После создания сайта и размещения его на хостинге оперативному сотруднику необходимо, например, включить инструмент AWstats. AWstats – инструмент веб-аналитики, который будет собирать статистику о трафике на сайте и о посетивших сайт пользователях[2]. На данный момент не только REG.RU, но и большинство хостинг-провайдеров предоставляют такой инструмент веб-аналитики, как AWstats.

Все эти данные могут обрабатываться и сохраняться в режиме реального времени. При этом оперативному сотруднику не обязательно постоянно наблюдать за конкретным пользователем. Нужно создать такие условия, чтобы киберпреступник перешел на сайт, созданный оперативным сотрудником. Например, при размещении объявления о продаже товара, запрещенного законом к продаже, продавцу необходимо отправить ссылку на сайт, созданный оперативным сотрудником, с фотографией касаемо уточнения наличия именно такого товара у пользователя. После этого, зайдя в интерфейс программы AWstats,

[1] Зарегистрировать домен [Электронный ресурс]. – URL: https://www.reg.ru/domain/new (дата обращения: 30.01.2025).

[2] What is AWStats [Электронный ресурс]. – URL: http://www.awstats.org (дата обращения: 03.02.2025).

программа покажет, когда и с какого IP-адреса осуществлялся переход на сайт. Это даст возможность оперативному сотруднику, не имея полного доступа к сайту, при помощи которого мошенник совершает противоправные действия, оперативно установить метаданные, а именно время перехода и IP-адрес компьютера, с которого осуществлялся переход киберпреступником по ссылке. Полученные данные позволят значительно сузить круг поиска подозреваемого. Также не нужно забывать, что при использования фишингового сайте не нужно допускать провокации со стороны сотрудников правоохранительных органов.

После того, как сотруднику стал известен IP-адрес компьютера, он должен установить принадлежность данного IP-адреса к провайдеру. Для этого хорошо подойдет бесплатный сайт http://2whois.ru/, который покажет, какому провайдеру принадлежит запрашиваемый IP-адрес, физический адрес провайдера и его владельца с контактным телефоном. Сотруднику ОВД останется направить мотивированный запрос провайдеру для предоставления анкетных данных владельца IP-адреса в соответствии с установленными законом процедурами.[1]

Рассматривая способы, которые используют злоумышленника в совершении преступлений, отдельно стоит остановиться на использовании искусственного интеллекта. Например, при помощи искусственного интеллекта, а именно технологии «deepfake» стало возможным создавать высококачественный медиаконтент (фото, видео, аудио), который выглядит как настоящий, хотя на самом деле является подделкой.

Число преступных схем с использованием «дипфейков», а именно случаев, когда преступники с целью выдать себя за другого человека методом синтеза подменяют его стилистику, поведение, тембр голоса, с начала 2024 года выросло в 30 раз. Убытки россиян от кибермошенничества, по оценкам аналитиков Сбербанка, по итогам 12 месяцев могли составить 300 млрд руб.[2] Распознать преступление, совершаемое с использованием «дипфейков», без использования

[1] Павлюков В.В. Компьютерная разведка как оперативно-розыскное мероприятие // Вестник Нижегородской академии МВД России. – 2016. – № 4(36). – С.239-240.

[2] Дипфейки идут на повышение [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/6962962 (дата обращения: 19.02.2025).

специальных программных продуктов практически невозможно. Искусственный интеллект – это новая форма современных специальных знаний, самообучаемая система, способная решать важные криминалистические задачи[1].

При расследовании преступлений, где медиафайлы («дипфейки») используются как средство (предмет) совершения преступления, отдельные ученые предлагают использовать методы для выявления внесённых технических изменений в исходную запись. Наряду с проверкой аутентичности медиаконтента, при расследовании могут использоваться методы аутентификации с применением искусственного интеллекта. Практика применения такого подхода может позволить усовершенствовать методики определения подлинности медиафайлов и использовать в криминалистических экспертизах[2].

Д. М. Берова и А.Ю. Тутуков приходят к выводу, что внедрение технологий искусственного интеллекта в процесс расследования и раскрытия преступлений имеет ряд неоспоримых преимуществ:

- за счет автоматизации сбора и обработки информации значительно сокращается время, необходимое для расследования преступления;

- возможность более точного анализа и оценки доказательств, обработки огромных массивов данных (например, о звонках, финансовых операциях, данных с камер наблюдения) повышает вероятность раскрытия преступления, способствует выявлению скрытых связей и паттернов в данных (например, между подозревамыми, жертвами, местами преступления и др.), которые могли бы остаться незамеченными с использованием традиционных методов;

- создание криминальных портретов, описывающих вероятные характериститки, психотипы и поведение преступников, позволяет ориентировать расследование на конкретных подозреваемых, вырабатывать наиболее подходящие тактические приемы осуществления следственных действий[3].

---

[1] Пристансков В.Д., Харатишвили А.Г., Евстратова Ю.А. Искусственный интеллект - новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений // Всероссийский криминологический журнал. – 2023. – Т. 17. – № 6. – С. 589 592.

[2] Исакова А.Г., Осин А.В. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «Дипфейк» // Вестник науки. – 2024. – Т. 3. – № 1 (70). – С.240-241.

[3] Берова Д.М., Тутуков А.Ю. Потенциал искусственного интеллекта в расследовании преступлений: за или против // Социально-политические науки. – 2024. – Т. 14. – № 3. – С. 98.

Подводя итоги параграфа, заметим, что, обладая специальными знаниями в сфере компьютерных технологий, специалисты способны внести неоценимый вклад в деятельность следователя по установлению истины при расследовании преступлений, совершаемых в области информационных технологий. Вместе с тем очевидным является тот факт, что расследование преступлений, совершаемых в сфере компьютерной информации, без разработки и внедрения современных программных продуктов и использования искусственного интеллекта, на современном этапе видится мало эффективным. Очевидно, что использование программных продуктов требует, как выбора тактик и методик их применения, так и законодательной регламентации возможности совмещения накопленной информации из сети Интернет с информацией, которая хранится в системе информационно -аналитического обеспечения МВД России.

ГЛАВА 3. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

§ 3.1. Организационно-тактические особенности расследования преступлений, совершаемых с использованием компьютерной информации

Человек является высшей социальной ценностью, а его права и свободы должны определять содержание и направленность деятельности государственных институтов. В этой связи оперативно-розыскная деятельность может рассматриваться как один из государственных правоохранительных механизмов, обеспечивающих защиту прав и свобод человека от противоправных посягательств, а также неотвратимость наказания для тех, кто совершает преступления, в частности, и в сфере обращения компьютерной информации.

Тактика проведения мероприятий, направленных на получение компьютерной информации в целях противодействия преступности, в современных условиях развития общества становится необходимым действием. На одном из совещаний, посвященном мерам повышения информационной безопасности, Д.А. Медведев прямо указал на то, что по некоторым оценкам мировые потери от преступности в сфере компьютерной информации составляют до полутриллиона долларов. Подсчитать их очень сложно, потому что, либо не все потери фиксируются, либо не о всех потерях заявляется. В России ущерб от такого рода преступлений тоже растет, а их значительное количество остаётся вне поля зрения правоохранительных органов из-за высокой их латентности[1]. Опыта и сил противостоять этому явлению явно недостаточно. Нужны новые действенные меры[2].

Как указывалось ранее, преступления в сфере компьютерной информации относятся, преимущественно, к категории латентных. Из-за несовершенства

[1] Куликов А.Г., Лазаревич В.В. О понятии и классификации способов совершения цифровых преступлений // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 1 (15). – С.70.

[2] Медведев оценил в полтриллиона долларов ущерб от киберпреступлений в мире. [Электронный ресурс] Интерфакс. – URL: http://www.interfax.ru/business/511660 (дата обращения: 22.02.2025).

существующих методик выявления таких противоправных деяний в поле зрения оперативно-розыскной деятельности в настоящее время попадают, главным образом, преступные деяния, не представляющие большой общественной опасности, не сложные по механизмам их выявления и раскрытия, а также расследования и доказывания[1].

В силу указанных причин становится понятным, что компьютерная среда с циркулирующей в ней информацией привлекает к себе не только добросовестных лиц, но и субъектов, склонных к занятию преступной деятельностью. Поэтому, обращая внимание на факт того, что современный криминальный мир сегодня уже не мыслит своего функционирования без компьютерных технологий, отдельные авторы, на наш взгляд, обосновано указывают на целесообразность проведения соответствующих оперативно-розыскных мероприятий в компьютерной сети, что, несомненно, положительно повлияет на предупреждение и предотвращение различных угроз для российского государства[2].

Для выяснения вопросов, связанных с распространенностью и выявлением отдельных видов преступлений при помощи ОРМ в Интернете, А.М. Ишиным было проведено анкетирование среди оперативных сотрудников. На вопрос: обращались ли Вы к Интернету за информацией по оперативным делам? – 21% респондентов ответили, что очень часто. 36,8% опрошенных лиц заявили о том, что неоднократно обращались в Интернет с целью поиска соответствующей информации.

Также было установлено, что в 75% случаев обращения респондентов в сеть Интернет нужная информация ими находилась лишь частично. Почти никогда не находили нужную информацию всего лишь 10% опрошенных. Причины неудач в поиске информации разнообразны, респонденты называли следующие: 1) отсутствие доступа к нужным сайтам и базам данных (63,6%); 2) отсутствие

---

[1] Александров И.В. Проблемные аспекты формирования методики расследования современных преступлений, совершаемых в сфере экономики // Вестник Московского университета. Серия 11: право – 2014. – № 4. – С. 38.

[2] Алябьев А.А., Лагуточкин А.В. Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет // Проблемы правоохранительной деятельности. – 2013. – № 1. – С. 67.

методики поиска соответствующей информации (22,7%); 3) необходимость использования специального программного обеспечения (13,6%)[1].

Такое разнообразие ответов свидетельствует, на наш взгляд, о том, что отдельные оперативные сотрудники ОВД еще не в полной мере осознают потенциал компьютерных сетей и систем, который предоставляет возможности получать оперативно значимую информацию.

Преимущества работы в процессе осуществления ОРД с компьютерной информацией могут принести положительный результат и, причем, в достаточно короткие сроки, ведь, если знать, чем интересуется пользователь компьютерной сети, то появляется возможность спрогнозировать его действия и впоследствии не только раскрыть, но и предвидеть преступление. В свою очередь, если такая деятельность носит явно противозаконный характер, компьютерную информацию необходимо получать незамедлительно и оперативно, прибегнув при этом к получению информации из источников с ограниченным доступом, то есть из таких, где доступ ограничен владельцем ресурса.

Принимая во внимание вышесказанное, стоит рассмотреть существующие правовые механизмы выявления правонарушителей, использующих в своих преступных целях возможности компьютерных технологий. И здесь, в первую очередь, целесообразно начать с анализа содержания положений ФЗ «Об оперативно-розыскной деятельности», акцентировав внимание при этом на том, что, когда Госдума РФ приняла поправки Яровой[2], на основании которых в ФЗ «О внесении изменений в ФЗ «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 № 374-ФЗ[3] были внесены изменения в ст. 6 ФЗ «Об

[1] Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. – С. 120.

[2] Госдума приняла антитеррористический пакет Ирины Яровой [Электронный ресурс]. – URL: http://pravo.ru/news/view/130575 (дата обращения: 26.02.2025).

[3] 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»: Федеральный закон от 06 июля 2016 № 374-ФЗ

оперативно-розыскной деятельности», последняя была дополнена пунктом 15-ым под названием «Получение компьютерной информации». Указанное ОРМ дополнило арсенал правоохранительных средств, с помощью которых оперативный сотрудник может получить оперативно-значимую информацию из компьютерных систем и сетей. Речь идет также о:

- контроле почтовых отправлений, телеграфных и иных сообщений;
- прослушивании телефонных переговоров;
- снятии информации с технических каналов связи.

Соответствующий потенциал за ОРМ «Контроль почтовых отправлений, телеграфных и иных сообщений» признают 17 % опрошенных, за ОРМ «Прослушивание телефонных переговоров» – 87 % респондентов, за ОРМ «Наведение справок» - 92 %, а за ОРМ «Снятие информации с технических каналов» – 70% проинтервьюированных сотрудников ОВД[1]. Показателен тот факт, что указанные мероприятия наряду с ОРМ «Получение компьютерной информации» действующие оперативные сотрудники считают также эффективными при получении оперативно-значимой информации из компьютерных систем.

Сказанное позволяет высказать суждение о том, что необходимо более четко обозначить роль и место ОРМ при получении компьютерной информации в процессе расследования преступлений.

Начнем с рассмотрения ОРМ «Наведение справок». В ходе опроса сотрудников ОВД установлено, что данное ОРМ оперативными сотрудниками проводится наиболее часто. Рассматриваемое мероприятие осуществляется путем направления запросов, при этом, по мнению А.А. Шмидта, не имеет существенной разницы, в какой именно форме выполняется запрос (устно, оформлен документально, запрос по каналам электронной почты). Источником информации при наведении справок могут являться как правоохранительные органы, так и предприятия, учреждения, организации, независимо от формы собственности,

---

[Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

[1] См.: Приложение № 1. Опросный лист.

располагающие необходимой информацией, а также физические лица и информационные базы данных[1]. Данное мероприятие может проводиться на любой стадии расследования и, на первый взгляд, не вызывает особых затруднений у сотрудников ОВД, в частности по той причине, что не требуют судебного санкционирования. Однако стоит учитывать, что запрашивать информацию о лицах, которая хранится в не ведомственных базах данных, стоит с осторожностью. Субъект, к которому поступил запрос, может проинформировать об этом лицо, в отношении которого запрашивалась информация. В таких ситуациях тактическим приемом может быть запрос не о лице, а об обстоятельствах и фактах, указывающих на необходимое лицо или нескольких лиц. В свой черед, направление запроса может привести к тому, что после его получения владелец информации по разным причинам может удалить запрашиваемую информацию и проинформировать лишь об ее отсутствии. Поэтому не всегда стоит получать компьютерную информацию путем направления запроса, иногда полезно будет личное участие или использование других ОРМ, при помощи которых возможно если не полностью, то максимально законспирировать запрашиваемую информацию.

По этим причинам стоит рассмотреть и иные ОРМ, направленные на получение компьютерной информации, где одним из наиболее актуальных и в то же время дискуссионных является «Получение компьютерной информации». Отдельные ученые заметили, что руководство Федеральной Службы Безопасности России (далее – ФСБ) в ведомственных разъяснениях к ФЗ от 6 июля 2016 г. № 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» высказало предположение, что мероприятие «Получение компьютерной информации», которое должно проводиться по решению суда соответствующими оперативно-техническими подразделениями,

[1] Шмидт А.А. К вопросу о классификации ОРМ «Наведение справок» // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2006. – № 6. – С. 67-69. – С. 69.

сможет позволить осуществлять копирование компьютерной информации, ее изъятие с жестких дисков сетевых компьютеров или серверов в информационно-телекоммуникационной сети Интернет, в том числе из «облачных» хранилищ - т. е. информация может быть получена путем удаленного доступа к компьютеру или серверу в сети Интернет[1].

С позиций оперативно-розыскной науки и практики А.Л. Осипенко выдвигает свою версию о содержании ОРМ «Получение компьютерной информации». Анализируя положения ФЗ «Об оперативно-розыскной деятельности», ученый указывает на то, что законодатель вряд ли связывает его с простейшими формами обращения к компьютерным ресурсам, находящимся у операторов связи или в открытом доступе, либо к устройствам хранения компьютерной информации, полученным в распоряжение субъектов оперативно-розыскной деятельности. Основу ОРМ «Получение компьютерной информации», по мнению А.Л. Осипенко, должны составлять достаточно сложные в техническом плане и требующие специальной подготовки действия по добыванию хранящейся в компьютерных системах или передаваемой по техническим каналам связи информации о лицах и событиях, вызывающих оперативный интерес[2].

По мнению Е.С. Дубоносова, получение компьютерной информации должно представлять оперативно-техническое мероприятие, направленное на сбор сведений, хранящихся в отдельном компьютере или циркулирующих в компьютерной сети, а также содержащихся на различных носителях машинной информации с последующей их фиксацией (или без неё) для решения оперативно-розыскных задач[3].

Как можно заметить, мнения ученых и практиков расходятся, и чтобы в дальнейшем урегулировать данные разногласия, целесообразно более конкретно рассмотреть отличительные признаки ОРМ при помощи которых возможно

---

[1] Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России, 2017. – №. 2 (65). – С. 31.

[2] Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. – 2016. – № 3. – С. 86.

[3] Дубоносов Е.С. Оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и проблемы проведения // Известия ТулГУ. Экономические и юридические науки. – 2017. – № 2-2. – С. 25.

получить значимую для расследования компьютерную информацию.

Для освещения данных вопросов очень часто прибегают к классификации, предложенной В.Г. Бобровым, где ОРМ предлагается разграничить по следующим признакам[1].

1. По продолжительности проведения. Исходя из данного признака, получение компьютерной информации при помощи ОРМ может быть, как длящееся, так и разовое. Это зависит от ряда обстоятельств. Так, например, если лицо ранее совершало преступления и использовало в своей деятельности компьютерную сеть, то, чтобы получить данные о его деятельности, возможно сделать разовый запрос к владельцу интернет-ресурса, провайдеру или оператору связи. Здесь будет не лишним обозначить и вид предоставления информации – последняя должна быть предоставлена в читабельном для просмотра оперативного сотрудника ОВД электронном виде (например, в word-документе в виде справки).

Получение компьютерной информации может также проводиться в течение длительного времени, но срок этот ограничен 6 месяцами, о чем указано в ст. 9 ФЗ «Об оперативно-розыскной деятельности». При необходимости продления срока судья выносит судебное решение на основании вновь представленных материалов. Здесь также интересен вопрос возможностей доступа к информации, который будет раскрыт далее.

2. В зависимости от формы проведения. Получение компьютерной информации зачастую осуществляется в ходе негласных ОРМ, то есть, когда об их проведении не знают посторонние лица и граждане, в отношении которых они проводятся, поскольку об их проведении может стать известно лицу, предоставляющему услуги телекоммуникации, которое, в свой черед, не является субъектом правоохранительной деятельности. Также результаты, полученные без ведома заинтересованных лиц, в дальнейшем могут быть преданы гласности.

С целью защиты интересов государства правоохранительные органы вынуждены в противодействии преступности наряду с гласными использовать и

[1] Бобров В.Г. Понятие оперативно-розыскных мероприятий. Основания и условия проведения оперативно-розыскных мероприятий: Лекция. – М.: Академия управления МВД России. – 2003. – С. 23-24.

негласные оперативно-розыскные мероприятия. Это связано, помимо прочего, еще и с высокой степенью конспирации при подготовке и совершении преступлений, особенно если речь идет о человеческой жизни и безопасности государства[1].

3. В зависимости от необходимости санкционирования. Практически все ОРМ (кроме «Наведение справок»), связанные с получением информации из компьютерных систем и сетей, а также у владельцев такой информации, законодатель отнес к таким, проведение которых требует судебного решения, о чем указано в ст. 8 ФЗ «Об оперативно-розыскной деятельности». Согласно требованиям данной статьи, проведение любых ОРМ, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации:

1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно;

2) о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно;

3) о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

По выше обозначенным аспектам нормативного регулирования проведения ОРМ среди практиков и ученых идет живая дискуссия, поэтому данный вопрос требует более детального рассмотрения. Ведь помимо того, что провайдеров обязали хранить компьютерную информацию, такая информация может храниться в учреждениях и организациях, внутри которых также может циркулировать большой объем компьютерных данных. Законодатель упустил из внимания тот

[1] Вахрушев С.Ю., Дмитриева А.А. Прослушивание телефонных переговоров как разведывательное оперативно-техническое мероприятие // Вестник ЮУрГУ. Серия: Право. – 2006. – № 13. – С. 35.

факт, что именно доступ к информации не всегда ограничен и это ставит под сомнение необходимость судебного санкционирования (например, системный администратор в организации не закрыл доступ к данным на сервере). Поэтому данный вопрос пока еще остается открытым для обсуждения и принятия по нему компромиссного решения.

Поскольку в правоохранительной практике часто необходимо проводить ряд действий по получению компьютерной информации, направленной на установление личности преступника, его связей, мест, средств, при помощи которых он осуществлял свою противоправную деятельность, а также устанавливать возможные каналы связи, используемые для обмена данными, то, на наш взгляд, получение компьютерной информации стоило бы проводить также в зависимости от имеющихся данных о факте совершаемого преступления и до момента его совершения. Такую возможность для правоохранительных органов РФ целесообразно было бы закрепить на законодательном уровне, поскольку отсутствие последней приводит к тому, что сотрудник правоохранительных органов не может в полной мере использовать потенциал компьютерной сети для получения из нее оперативно значимой информации на момент совершения преступления.

В спектре определения возможных направлений разрешения указанных проблем, напомним, что в условиях современного этапа развития компьютерных информационных систем компьютерную информацию уже можно получать как из открытых источников, так и из источников с ограниченным доступом. Считаем, что первоначальный интерес представляют открытые источники информации в плане использования их возможностей в деятельности по раскрытию и расследованию преступлений, в частности, для получения криминалистически значимой информации.

Р.С. Белкин отмечает, что «криминалистически значимой может оказаться любая информация любой природы»[1]. Поддерживая эту точку зрения, отметим, что открытые источники являются ценным носителем криминалистически значимой

[1] Белкин Р.С. Криминалистическая энциклопедия. – М.: Мегатрон XXI, 2000. – 2-е изд. доп. – С. 84.

информации и являются пространством для проведения ОРМ. Причем известно, что 80-90% разведданных можно получить через открытые источники, в том числе компьютерную сеть. Поэтому, с учетом прогрессивного развития информационно-телекоммуникационных технологий и стремительного роста количества открытых источников информации во всем мире, полагаем, что открытые источники информации уже превратились в уникальную силу и средство борьбы с преступностью, так как имеют неограниченные возможности и потенциал для проведения в них ОРМ.

А.М. Ишин обращает внимание на то, что наличие в сетевом пространстве криминогенной среды является основанием как для проведения розыскной, так и поисковой деятельности органами предварительного следствия[1]. Оперативные работники в ходе выполнения служебных обязанностей по установлению первичных данных о лицах, фактах и местах, которые позволяют выявить противоправные действия из открытых источников, должны начинать свою деятельность с осуществления оперативного поиска, используя компьютерные системы, программное обеспечение, а также интернет-ресурсы.

Оперативный поиск направлен на выявление в окружающей среде, в том числе и в сети Интернет, информации о лицах, которые имеют непосредственное отношение к подготовке или совершению противоправных действий путем использования компьютерных систем, после чего остаются цифровые следы от их действий на различных электронных носителях. Оперативный поиск информации – это непрерывный процесс, который осуществляется постоянно с целью выявления ранее неизвестных сотрудникам оперативных подразделений лиц, от которых можно ожидать совершения противоправных действий в компьютерных сетях и системах, или фактов, которые свидетельствуют о намерениях, подготовке или совершении таких преступлений.

Оперативный поиск можно считать также первой стадией оперативно-розыскного процесса, которая имеет свою особую правовую природу, основания и

[1] Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. – С. 120.

принципы. Результаты оперативного поиска могут использоваться для проведения иных оперативно-розыскных мероприятий в соответствии с нормативными положениями части 1 ст. 11 ФЗ «Об оперативно-розыскной деятельности»[1].

Главным предназначением оперативного поиска является то, что он призван помогать оперативным подразделениям обнаруживать не только неизвестных лиц, которые представляют оперативный интерес, но также и факты, указывающие на преступные намерения, подготовку или уже совершенные противоправные действия, связанные с получением и использованием компьютерной информации со стороны конкретных граждан, в том числе тех, которые уже находятся под наблюдением оперативных служб.

Как видим, основной задачей оперативного поиска является выявление еще неизвестных фактов преступлений, а также лиц, их совершивших. Другой отличительной чертой оперативного поиска является его организация в местах наиболее вероятного обнаружения объектов. Такая вероятность появляется там и тогда, когда криминогенные процессы в определенных условиях имеют тенденцию повторяемости, регулярности проявления во времени и пространстве. Наличие сведений о неоднократно совершаемых в определенном месте правонарушениях служит достаточным основанием для прогнозирования вероятности совершения там новых общественно опасных деяний, а также для проведения в таком месте в соответствии с п. 2 ст. 7 ФЗ «Об оперативно-розыскной деятельности» оперативно-поисковых мероприятий с целью выявления лиц, подготавливающих, совершающих или совершивших преступления, пресечения преступных деяний[2].

Оперативный поиск, связанный с выявлением оперативной информации в сетевом информационном пространстве о противоправных действиях, называют интернет-мониторингом, который представляет собой комплексную систему наблюдения за состоянием криминальных процессов в сетевой социальной среде, направленную на сбор, обработку и анализ информации о явлениях криминального

[1] Меретуков Г.М., Лунина Е.С., Липка А.О. Сущность и значение поисковой деятельности подразделений, осуществляющих оперативно-розыскную деятельность // Научный журнал КубГАУ - Scientific Journal of KubSAU. – 2016. – № 116. – С. 959.

[2] Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – М.: ИНФРА, 2006. – С. 447.

плана. Основными направлениями этого мониторинга, способными обеспечить высокую интенсивность поступления криминалистически значимой информации, являются поиск, изучение и наблюдение за ресурсами сети Интернет, где содержится указывающая на преступную деятельность информация[1].

После выявления в открытых источниках компьютерной информации, которая может свидетельствовать о совершении противоправных действий, сотрудник оперативного подразделения должен определиться с выбором ОРМ и тактикой его применения, направленной на получение данных из источников с ограниченным доступом.

Ранее мы отмечали, что отдельные ученые отождествляют ОРМ «Получение компьютерной информации» с такими мероприятиями, как «Снятие информации с технических каналов связи». Схожее мнение выразили и некоторые практики, у которых появление нового ОРМ «Получение компьютерной информации» породило бурные дискуссии на полицейских форумах сети Интернет. Часть пользователей, присоединившихся к форуму, считают, что получение компьютерной информации не что иное, как составляющая такого оперативно-розыскного мероприятия, как «Снятие информации с технических каналов связи». В частности, администратор форума «Skyment» указывает на следующее: «Простой запрос в поисковик подпадёт под данное ОРМ...»[2].

На наш взгляд, ОРМ «Получение компьютерной информации» не следует отождествлять с таким оперативно-розыскным мероприятием, как «Снятие информации с технических каналов связи». Согласно ст. 8 ФЗ «Об оперативно-розыскной деятельности» ОРМ «Снятие информации с технических каналов связи» точно также, как и «Получение компьютерной информации», допускается на основании судебного решения и при наличии ограниченного перечня оснований,

[1] Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – №. 9. – С.121.

[2] Форум сотрудников ОВД [Электронный ресурс]. – URL: https://www.police-russia.ru/showthread.php?p=3553535 (дата обращения: 12.01.2025).

указанных в этой статье[1]. Вместе с тем, в одном из научных комментариев к закону «Об оперативно-розыскной деятельности» разъясняется, что «Снятие информации с технических каналов связи» представляет собой негласный контроль, заключающийся в совокупности действий по получению оперативно значимых сведений, их фиксации путем съема специальными техническими средствами электромагнитных и других физических полей, возникающих при передаче информации по сетям электронной связи, в работе компьютерной сети, баз данных, телекоммуникационных систем[2].

Другие ученые обращают внимание на то, что обмен письмами, как информационными сообщениями, подразумевает разрыв во времени между передачей сообщения и получением его лицом, которому такое сообщение предназначено, и воспринимается через орган зрения. Именно разрыв во времени позволяет наложить арест на носитель информации, произвести его осмотр и выемку, что невозможно при непосредственном обмене речевыми сообщениями. Компьютерные технологии информационного обмена совмещают в себе особенности «привычных» видов коммуникации. Сообщения электронной почты, как правило, находятся на сервере до того момента, пока пользователь не получит их. После этого такие сообщения удаляются[3].

Дополнительно стоит акцентировать внимание также и на том, что отличительным признаком снятия информации с технических каналов связи является перехват данных, которые передаются по компьютерным сетям, где в отличии от привычной передачи бумажного письма, цифровое сообщение передается за доли секунд и зачастую является зашифрованным. Также нужно знать место, откуда будет происходить отправка данных, а в случае с компьютерной информацией это может быть сделано как при помощи оператора

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп.) [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[2] Дубягин Ю.П., Дубягина О.П., Михайлычев Е.А. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» (постатейный). – [Электронный ресурс]. – URL: https://www.lawmix.ru/commlaw/1518 (дата обращения: 24.02.2025).

[3] Кузченко Д.В., Кушпель Е.В. О некоторых тактических особенностях поиска, фиксации и изъятия компьютерной информации в ходе наложения ареста на почтово-телеграфные отправления и при контроле и записи переговоров // Вестник Барнаульского юридического института МВД России. – 2011. – № 1(20). – С. 40.

мобильной связи, так и при помощи различных интернет-провайдеров, что весьма затрудняет осуществление такого ОРМ как «Снятие информации с технических каналов связи».

Схожая ситуация и с ОРМ «Прослушивание телефонных переговоров». Оно тоже допускается только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, лиц, которые могут располагать сведениями об указанных преступлениях[1]. Данное ОРМ может проводиться также по письменному соглашению потерпевших, свидетелей, их близких родственников, близких лиц – при наличии угрозы совершения против них преступных действий. При этом нужно понимать, что в первом случае целью контроля и записи переговоров является получение доказательственной информации по делу; во втором – защита перечисленных лиц от преступных посягательств[2].

На наш взгляд, не следует отождествлять ОРМ «Контроль почтовых отправлений, телеграфных и иных сообщений» также с таким мероприятием, как «Получение компьютерной информации» и «Прослушивание телефонных переговоров». Судебные решения, в которых говорилось о проведении компетентными органами ОРМ «Контроль почтовых отправлений, телеграфных и иных сообщений», указывают на то, что данное мероприятия в большинстве случаев использовалось только с целью вскрытия посылок в почтовых отделениях. В частности, вот один из примеров, который подтверждает сказанное. Так гр. Х., посредством почтовой связи незаконно переслал гр. Н. наркотическое средство в крупном размере. На основании постановления судьи Верховного суда «О разрешении проведения оперативно-розыскного мероприятия «Контроль почтовых отправлений, телеграфных и иных сообщений» в отношении почтовых отправлений, поступивших по адресу отделения почтамта, в помещении почтамта было вскрыто поступившее почтовое отправление (конверт). При вскрытии

[1] Дытченко Г.В., Никитин Е.Л. Законность проведения оперативно-розыскных мероприятий, ограничивающих конституционные права граждан // Криминалист. – 2011. – № 1(8). – С. 103.

[2] Дунаева М.С. Проблемы защиты частной жизни граждан при осуществлении контроля и записи переговоров // Адвокатская практика – 2003. – № 3. – С. 16.

указанного конверта внутри него были обнаружены: 1) одна открытка с надписью: «В день рождения! Душевного тепла и процветания!»; 2) 2 бумажных пакета с порошкообразным веществом жёлтого цвета, приклеенные липкой лентой к внутренней стороне открытки[1].

Необходимо заметить, что выше обозначенные ОРМ являются длительными по времени и не всегда дают положительный результат. В частности, преступники активно используют различные средства и методы шифрования компьютерной информации[2], отказываются от сотовой связи, контактируют через Интернет, что снижает эффективность таких классических мероприятий, как прослушивание телефонных переговоров, контроль почтовых, телеграфных и иных сообщений и т. п.[3]

Упускается и тот момент, что в сервисах сети Интернет легко реализовать возможность скрыть информацию о себе. Ведь, как известно, чтобы безнаказанно осуществлять свою противоправную деятельность, лицо дезинформирует других пользователей, используя вымышленные анкетные данные и адреса, тем самым пытается скрыть свои следы[4], которые прямо указывали бы на него.

Тактическим приемом будет совместное проведение таких мероприятий, как получение компьютерной информации, контроль почтовых отправлений, телеграфных и иных сообщений, а также снятие информации с технических каналов связи. Считаем, что компьютерная информация, полученная при помощи рассматриваемых ОРМ в процессе расследования преступлений, будет также иметь и процессуальное значение, если их осуществление будет происходить в связке т.е., когда они смогут дополнять друг друга. Анализ судебной практики показывает, что

---

[1] Приговор Останкинского районного суда по ч. 3 ст. 228.1 УК РФ № 1-278/2015 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/82963.html (дата обращения: 08.02.2025).

[2] Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / Зиновьева Нина Сергеевна. – Краснодар. – 2020. – С.152.

Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / Касаткин Андрей Валерьевич. – М., 1997. – С 17.

[3] Законодательство об оперативно-розыскной деятельности отстает от жизни: интервью с Сергеем Викторовичем Ивановым, начальником управления по надзору за производством дознания и оперативно-розыскной деятельностью Генеральной прокуратуры РФ // Уголовный процесс. – 2016. – № 3. – С. 30.

[4] Алиева Г.А., Кустов А.М. Получение криминалистически значимой информации из мессенджера Whatsapp в качестве источника доказательственной информации // В книге: Проблемы получения и использования доказательственной и криминалистически значимой информации. материалы Международной научно-практической конференции. – 2019. – С.3.

факт совместного использования таких мероприятий при раскрытии и расследовании преступлений неоднократно приносил свои положительные результаты. Доказательством тому являются соответствующие примеры. В частности, в деле Сакмарского районного суда № 1[1]-21/2017 от 25 июля 2017 г. говорится о том, что сотрудниками УФСБ России в отношении гр. Щ., с целью проверки оперативной информации о его причастности к совершению противоправных действий, связанных с организацией незаконного пребывания в РФ иностранных граждан, проводились такие ОРМ, как «Прослушивание телефонных переговоров», «Снятие информации с технических каналов связи» и «Контроль почтовых отправлений, телеграфных и иных сообщений». В результате прослушивания переговоров гр. Щ. была выявлена информация о причастности последнего к противоправной деятельности, связанной с мошенническими действиями в отношении потерпевшего, в связи с чем, в отношении него по результатам ОРМ «Прослушивание телефонных переговоров» возбуждено уголовное дело[1].

Сотрудники ОВД тоже заявляют о необходимости совместного проведения соответствующих ОРМ. В частности, 83 % респондентов высказались за то, чтобы такие ОРМ, как «Получение компьютерной информации» и «Снятие информации с технических каналов связи» всегда осуществлялись совместно. Не поддержали указанную идею только 17 % опрошенных сотрудников[2].

Однако существуют обстоятельства, когда реализация указанных ОРМ может быть нерезультативной. Это происходит тогда, когда оператор связи, провайдер, владелец ресурса компьютерной сети отказывается предоставлять доступ к своим ресурсам. Препятствием выступает и то, что ресурс или техническое средство, представляющие оперативный интерес, защищены паролем. Подтверждает данные суждения диалог владельца Telegram Павла Дурова с Роскомнадзором. В частности, Глава Роскомнадзора заявил, что владелец Telegram должен выдать спецслужбам «ключи для дешифрации», чтобы те могли читать переписку

[1] Приговор Сакмарского районного суда Оренбургской области № 1[1]-21/2017 от 25 июля 2017 г [Электронный ресурс]. – URL: http://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/28593136 (дата обращения: 08.02.2025).

[2] См.: Приложение № 1. Опросный лист.

пользователей и выявлять террористов. Однако П. Дуров отметил, что подобное требование не только противоречит ст. 23 Конституции РФ о праве на тайну переписки, но и демонстрирует незнание того, как шифруется коммуникация. Также он обратил внимание на то, что обмен секретной информацией построен на оконечном шифровании, к которому у владельцев мессенджеров нет и не может быть «ключей для дешифрации». Эти ключи хранятся только на устройствах самих пользователей[1].

Осознавая это, 92 % опрошенных оперативных сотрудников солидарны с тем мнением, что в неотложных случаях допустимо осуществлять действия по получению компьютерной информации без предварительной санкции, но с последующим судебным санкционированием, и только если есть основания полагать, что такая информация имеет оперативное значение при раскрытии и расследовании преступлений. 2 % респондентов высказались против такого подхода, 6 % опрошенных затруднились ответить на данный вопрос[2].

Мы также считаем, что оперативное преодоление компьютерной защиты является необходимой мерой в целях получения компьютерной информации о противоправной деятельности[3], законность и целесообразность применения которой были обоснованы в параграфе 1.3 данного исследования и подтверждены международной практикой. В этой связи полагаем, что при работе сотрудников оперативных подразделений РФ необходимо применять такие оперативно-розыскные мероприятия, которые не требуют санкций от руководства или суда. Подобные действия будут способствовать повышению эффективности, экономии времени и средств при проведении ОРМ.

В поиске разрешения проблем, связанных с выявлением без судебного решения следов противоправной деятельности в сфере информационных технологий и установлением принадлежности пользователя, который оставил

---

[1] Дуров: блокировка Telegram не поможет в борьбе с терроризмом [Электронный ресурс]. – URL: http://www.ntv.ru/novosti/1826858/ (дата обращения: 27.01.2025).

[2] См.: Приложение № 1. Опросный лист.

[3] Швец С.В., Павлюков В.В. Преодоление средств компьютерной защиты как необходимый способ реализации оперативно-розыскного мероприятия «Получение компьютерной информации» // Общество: политика, экономика, право. – 2018. – № 6. [Электронный ресурс]. – URL: https://doi.org/10.24158/pep.2018.6.15/ (дата обращения: 20.01.2025).

такую информацию, стоит указать на то, что для начала необходимо получить и проверить информацию о факте совершения преступления при помощи ОРМ.

Пока такое мероприятие применительно к сфере компьютерных технологий не нашло законодательного закрепления, однако стоит отметить, что использование современных информационных технологий в ОРД уже порождает новые направления деятельности, такие, как разведка, а именно компьютерная разведка, которая неумолимо меняет весь облик оперативной работы[1].

В юридической литературе нет четкого понятия «разведка», однако некоторые исследователи рассматривают ее как теорию и практику сбора информации о противнике или конкуренте для безопасности и получения преимуществ в военной области, политике или экономике[2]. Стоит обозначить, что разведка заключается в осуществлении организационных и технических мероприятий по добыче информации о противнике и сложившейся обстановке. Проведя аналогию с военными разведывательными подразделениями, последние при осуществлении разведывательных мероприятий преодолевают различные трудности, связанные с защитой от проникновения к субъекту, в отношении которого проводится разведка. Сейчас такую разведку возможно провести не только на поле боя, но и в источниках Глобальной сети Интернет.

А.В. Мовчан под компьютерной разведкой подразумевает необходимое оперативно-поисковое мероприятие, заключающееся в целенаправленном поиске и получении информации из компьютерных систем и сетей, доступ к которым не ограничивается их собственником, владельцем либо держателем. Однако такой доступ также не связан с преодолением системы логической защиты[3].

Стоит также указать, что к открытым источникам относятся источники легально полученной информации, доступ к которым не ограничен законом. Легальность и законность рассматривается только в контексте юрисдикции

---

[1] Овчинский А.С. Информация и оперативно-розыскная деятельность: Монография / Под ред. заслуженного юриста Российской Федерации, доктора юридических наук, профессора В.И. Попова. – М.: ИНФРА, 2002. – С. 8.

[2] «Военная разведка» [Электронный ресурс] // Онлайн энциклопедия «Кругосвет». – URL: http://www.krugosvet.ru/enc/nauka_i_tehnika/ (дата обращения: 11.02.2025).

[3] Мовчан А.В. Отдельные аспекты применения компьютерной разведки в оперативно-розыскной деятельности // Проблемы правоохранительной деятельности. – 2014. – № 2. – С. 110.

(действующего законодательства) территории, на которой ведутся или планируются оперативные мероприятия[1].

Поэтому предложенная А.В. Мовчаном интерпретация рассматриваемого ОРМ «Компьютерная разведка» не отличает его от других мероприятий, посредством осуществления которых оперативный сотрудник может также искать и просматривать информацию в открытых источниках компьютерных систем и сетей. В связи с тем, что источники компьютерной информации бывают не только открытыми (общего доступа), но и такими, к которым доступ закрыт или ограничен, компьютерная разведка, нацеленная на добывание разведывательной информации из таких источников, видится весьма актуальной и тем самым отличается от других ОРМ. Компьютерная разведка, в отличие от других ОРМ, направлена на эффективное получение информации из защищённых источников, предусматривающее использование методов преодоления программной защиты, осуществляемое на законных основаниях. К объектам атаки при провидении компьютерной разведки относятся операционные системы, отдельные модули ОС (файловая система, файлы, устройства и т.д.), пользователи ОС, каналы передачи информации. Средствами атаки могут стать штатные средства ОС, ПО третьих фирм (компьютерные программы, которые можно найти в сети Интернет, специально разработанное ПО).[2]

Также необходимо понимать, что каждый, в отношении кого будет проводиться разведка, может предвидеть возможность осуществления в отношении себя соответствующих действий со стороны разведчика, на основании чего попытается приложить максимум усилий для защиты своей информации и обнаружения разведчика. Уже сейчас современные информационные технологии предоставляют тем или иным пользователям достаточное количество механизмов защиты их информации, чем, безусловно, пользуются как законопослушные

[1] Власов М.П., Голоскоков К.П., Черкова М.Ю. Технологии научных исследований в «сети корпоративных знаний» // Сборник научных трудов SWorld: Материалы международной научно-практической конференции «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании 2012». – Одесса, Куприенко, 2012. – № 4(30). – С. 6.

[2] Основы кибербезопасности : учебник / А.О. Авсентьев, С.А. Винокуров, М.М. Жуков [и др.]. – М. : ГУРЛС МВД России, 2024. – 408 с. С.258-259.

граждане, так и лица, склонные к совершению преступлений при помощи компьютерной сети. Более того, даже интернет-компании неохотно идут навстречу полиции. В частности, корпорация Google, неоднократно получающая от российских правоохранительных органов запросы о предоставлении сведений в отношении определенных правонарушителей-пользователей, еще ни разу их не удовлетворила[1]. Очевидно, что такое положение дел сводит на нет все возможности использования существующих ОРМ и повышает актуальность компьютерной разведки.

С.Л. Емельянов высказывает дискуссионное суждение о том, что основным методом ведения компьютерной разведки является несанкционированный доступ к компьютерной информации, циркулирующей в компьютерной сети (далее – КС). Способы бесконтактного несанкционированного доступа в КС основаны на использовании недостатков языков программирования, наличии уязвимостей (брешей, «люков», «дыр» и т. д.) в штатном программном обеспечении КС и применении специального программного обеспечения, называемого атакующим[2].

До сих пор нет единого научного подхода относительно роли и места компьютерной разведки в теории ОРД. Конечно же, это негативно отражается как на оперативно-розыскном законодательстве (ФЗ «Об оперативно-розыскной деятельности» такой дефиниции не содержит), так и на практике его применения. Такая ситуация требует скорейшего ее осмысления.

Значимость такого мероприятия, как компьютерная разведка в решении задач ОРД – очевидна. Оно может иметь весомое значение по той причине, что информация, которая получена в ходе данного мероприятия, может послужить основанием для дальнейших действий оперативного сотрудника. В последствии такие действия могут стать основанием для проведения таких ОРМ, как: «Получение компьютерной информации», «Снятие информации с технических каналов связи», «Прослушивание телефонных переговоров» и т. д. Компьютерная

[1] Google сотрудничает с силовиками [Электронный ресурс]. – URL: https://wek.ru/google-sotrudnichaet-s-silovikamihttps://wek.ru/google-sotrudnichaet-s-silovikami (дата обращения: 12.02.2025).

[2] Емельянов С.Л. Техническая разведка и технические каналы утечки информации // Одесская национальная юридическая академия. – 2010. – № 3(84). – С. 23.

разведка должна проводится как первоочередное мероприятие, с чем солидарны 54% опрошенных оперативных сотрудников[1].

При рассмотрении компьютерной разведки в сети необходимо учитывать, что публично размещенная информация, согласно позиции А.П. Сергеева, становящаяся всеобщим достоянием при свободном доступе[2], и находится в иной правовой плоскости, чем конфиденциальные данные. Однако информация, циркулирующая в сети, в целом находится в зоне правового регулирования, особенно в части защиты персональных данных и тайны коммуникаций.

Возникает вопрос: будет ли предложенное ОРМ нарушать конституционные права граждан? В юридической литературе существуют различные точки зрения, например, вывод Е.В. Митина о том, что при использовании вымышленных данных в электронном почтовом ящике отсутствует объект преступления по ст. 138 УК РФ, а следовательно, и нарушение конституционного права на тайну переписки[3]. Однако эта позиция не совсем правильная, поскольку право на тайну коммуникаций принадлежит любому человеку, независимо от его способности быть немедленно идентифицированным по реальным данным, и анонимность не лишает личность базовых прав на неприкосновенность частной жизни (ст. 23, 24 Конституции РФ). Доступ к содержанию таких коммуникаций, даже при наличии вымышленных данных, всегда требует строгой судебной санкции, так как затрагивает конституционно защищённые права.

Тем не менее, в исключительных случаях, не терпящих отлагательства, когда промедление с получением компьютерной информации может привести к совершению тяжкого преступления, угрозе жизни или уничтожению доказательств, допустимо немедленное получение такой информации с обязательным последующим уведомлением суда и получением санкции в строго установленные законом сроки. Это обеспечивает необходимый баланс между эффективностью оперативно-розыскной деятельности и конституционными

[1] См.: Приложение № 1. Опросный лист.

[2] Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. – М.: Теис, 1996. – С. 621.

[3] Митин Е.В. Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации // Теория и практика общественного развития. – 2012. – № 9. – С. 272.

гарантиями прав граждан.

Именно в таких ситуациях компьютерная разведка становится незаменимым ОРМ, дающим возможность не только наблюдать, но также, при строгом соблюдении процессуальных норм, преодолевать средства компьютерной защиты и получать доступ к оперативно значимой информации. Такая особенность компьютерной разведки, основанная на современных технологиях целевого и санкционированного проникновения в информационное окружение, принципиально отличает её от других ОРМ, таких как поиск и получение компьютерной информации.

С учетом указанного, полагаем, что перечень оперативно-розыскных мероприятий, обозначенных в ст. 6 ФЗ «Об оперативно-розыскной деятельности», необходимо дополнить таким самостоятельным ОРМ, как «Компьютерная разведка». Под последней следует понимать активные действия сотрудников правоохранительных органов России по получению компьютерной информации оперативно-розыскного значения путем преодоления компьютерной защиты (проведение SSRF-атак, SQL-инъекций, использование эксплойтов, поиск RCE-уязвимостей и т. п.) на удаленных интернет-ресурсах или же путем анонимного получения информации от злоумышленников при помощи сети Интернет. Реализация данных рекомендаций повысит эффективность получения дополнительной оперативно-значимой информации, позволяющей устанавливать криминальные связи преступника, его переписку и место нахождения последнего.

На законодательном уровне необходимо также будет закрепить дефиницию ОРМ «Получение компьютерной информации». По нашему мнению она могла бы иметь следующую интерпретацию: **Получение компьютерной информации** – это оперативно-розыскное мероприятие, направленное на получение информации из компьютерных устройств, программного обеспечения, ресурсов сети Интернет путем их осмотра в целях фиксации противоправной деятельности определенных субъектов без судебного решения из открытых интернет-ресурсов, а в случае, если доступ к источнику информации закрыт, то при наличии судебного решения или без него, но при добровольном согласии владельца компьютерной техники или

пользователя ресурса сети Интернет.

§ 3.2. Тактические особенности фиксации и использования компьютерной информации при осуществлении отдельных следственных действий

При проведении следственных действий для установления фактов, обстоятельств и вины конкретного лица, совершившего противоправное деяние при помощи информационных технологий, особое значение приобретают тактические особенности фиксации и использования компьютерной информации в рамках правового поля.

Начнем с того, что существенное значение для подготовки и осуществления следственных действий имеют материалы ОРМ, при помощи которых зафиксирована компьютерная информация. Материалы, получаемые в ходе ОРД, в УПК РФ в ст. 5 п. 36.1 носят название «результаты оперативно-розыскной деятельности», под которыми понимаются «сведения, полученные в соответствии с федеральным законом об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда»[1].

Результаты, полученные в ходе проведения любого ОРМ, должны быть не только отражены в материалах дела оперативного учета, но и легализованы для их дальнейшего использования в уголовном деле. Помимо прочего, положения ст. 11 ФЗ «Об оперативно-розыскной деятельности» предусматривают возможность использования результатов такой деятельности в качестве повода и основания для возбуждения уголовного дела. Также такие результаты могут использоваться в процессе доказывания[2].

Фиксация результатов ОРД регламентируется «Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания,

[1] Уголовно-процессуальный кодекс РФ от 18 декабря 2001 № 174-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

[2] Ефремов К.А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. – 2016. – № 6. – С. 93.

следователю или в суд», где в п.6 сказано, что результаты, полученные в ходе проведения ОРД, должны быть представлены в виде рапорта об обнаружении признаков преступления или сообщения о результатах оперативно-розыскной деятельности. Также в п. 16 Инструкции указано, что к рапорту могут прилагаться (при наличии) полученные (выполненные) при проведении ОРМ материалы фото- и киносъемки, аудио- и видеозаписи, а также иные носители информации и материальные объекты[1]. Считаем, что такими носителями информации могут быть, в частности, электронные носители информации с файлами скриншотов или скринкастов, сделанные в ходе проведения ОРМ «Получение компьютерной информации».

Однако существует точка зрения, что использование результатов ОРД для осуществления следственных действий носит преимущественно некий информационный фундамент и, по мнению С.Б. Россинского, не может быть применено в качестве доказательства[2]. В то же время А.У. Садыков отмечает, что следователь, чтобы иметь возможность использовать результаты ОРМ в качестве доказательств, обязан установить и зафиксировать их источники, соблюдая правила доказывания[3].

Среди распространенных следственных действий, при подготовке и проведении которых следует использовать компьютерную информацию, в том числе полученную в ходе ОРД, ученые зачастую выделяют осмотр[4] и допрос[5].

Осмотр. В п. 1 ст. 176 УПК РФ перечислены такие виды осмотров, как: осмотр места происшествия, местности, жилища, иного помещения, предметов и документов. Привлекательность и особенность осмотра, а именно осмотр места

---

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_155629/ (дата обращения: 19.02.2025).

[2] Россинский С.Б. Проблема использования в уголовном процессе результатов оперативно-розыскной деятельности требует окончательного разрешения // Lex Russica. – 2018. №. – 10 (143). – С.72.

[3] Добренко М.А. Возможности использования результатов оперативно-розыскного мероприятия «Опрос» в уголовном процессе // Историческая и социально-образовательная мысль. – 2015. – № 3(7). – С.109.

[4] Красненко Ю.В. Поисково-познавательная деятельность на первоначальном этапе расследования // Вестник Белгородского юридического института МВД России. – 2019. – №. 3. – С.53.

[5] Садыков А.У. Использование результатов оперативно-розыскной деятельности при подготовке и проведении допросов // Общество и право. – 2015. – № 3 (53). – С.193.

происшествия, документов и предметов, заключается в том, что он может быть произведен до возбуждения уголовного дела, о чем указано в п. 2 упомянутой статьи. Из п. 3 ст. 177 УПК РФ также известно, что, если следователь не может провести осмотр на месте или если для производства такого осмотра требуется продолжительное время, то предметы должны быть изъяты, упакованы, опечатаны, заверены подписью следователя на месте осмотра. Стоит подчеркнуть, что изымать разрешено только те предметы, которые могут иметь отношение к уголовному делу, при этом в протоколе осмотра, если есть возможность, необходимо отразить индивидуальные признаки и особенности изымаемых предметов.

Мы не будем детально останавливаться на таком следственном действии, как осмотр места происшествия и основаниях его проведения, а сконцентрируем свое внимание на тактических особенностях фиксации компьютерной информации, находящейся на конкретном предмете для дальнейшего ее использования.

При работе с компьютерной информацией, имеющей отношение к уголовному делу, и предметом (мобильным телефоном, планшетом, стационарным компьютером, сетевым оборудованием и т.д.), на которых содержится компьютерная информация, зачастую осуществляется такое следственное действие, как осмотр предметов. Особое внимание стоит уделить *подготовительному этапу*, а именно действиям, направленным на выяснение сущности информации, имеющей отношение к расследованию, которая может храниться на предмете до начала проведения его осмотра. Как правило, на данной стадии следователь может ознакомиться с уже имеющимися результатами ОРМ, если такие есть в наличии.

Проанализировав судебную практику, приходим к выводу, что фиксация компьютерной информации нередко запечатлена путем снимка экрана смартфона или монитора компьютера (скриншота)[1], который прилагается к рапорту, протоколу или акту. Стоит указать, что скриншоты возможно сделать при помощи одновременного нажатия на клавиатуре клавиш Ctrl+Print Screen, после чего

[1] Постановление Анапского городского суда (Краснодарский край) № 5-3613/2018 от 2 ноября 2018 г. по делу № 5-3613/2018[Электронный ресурс]. – URL: https://sudact.ru/regular/doc/iD75SkvOV7by/ (дата обращения: 11.02.2025).

скриншот сохраняется в памяти компьютера. На мобильном телефоне также возможно сделать скриншот. В зависимости от марки телефона скриншот делается по-разному. Как правило, осуществляется нажатие нескольких клавиш, например, на мобильном телефоне фирмы «Apple» необходимо одновременно нажимать кнопки «Домой» и «Питание». Сделанный снимок можно вставить как в графический редактор, так и в текстовый, после чего полученный результат распечатать.

Судебная практика также позволяет сделать вывод, что суды принимают «скриншоты» в качестве надлежащих доказательств, однако для использования их в этом качестве к ним должны предъявляться определенные требования, упоминание о которых, как пример, можно встретить в письме Федеральной налоговой службы от 31.03.2016 г. № СА-4-7/5589 «О понятии «скриншот»», а именно:

- на скриншоте необходимо проставить дату и время получения информации с сайта в сети Интернет;

- указать наименование сайта (полный URL-адрес интернет-страницы, с которой сделан скриншот);

- скриншот должен содержать данные о лице, которое произвело его выведение на экран и дальнейшую распечатку, а также сведения о программном обеспечении и использованной компьютерной технике[1].

Е.А. Денисова выделяет несколько способов оформления следователем скриншотов, а именно: помещение скриншотов непосредственно в описательную часть протокола осмотра; оформление скриншотов в виде фототаблицы к протоколу осмотра; прикладывание скриншотов как иного приложения к протоколу осмотра. Автор также отмечает, что скриншот должен быть сохранен на электронном носителе информации (например, CD-R диске)[2].

Однако полагаться на одни лишь скриншоты, сделанные оперативным

---

[1] Письмо Федеральной налоговой службы от 31 марта 2016 г. № СА-4-7/5589 О понятии «скриншот» («снимок экрана») и порядке его использования. [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71284846/ (дата обращения: 04.03.2025).

[2] Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. Вопросы студенческой науки. 2017. № 15. – С.183.

сотрудником, будет недостаточно. Как справедливо заметили В.Д. Еськов и С.А. Чеботарев, только лишь распечатанный скриншот не может являться доказательством в связи с тем, что он может быть самостоятельно создан в графических редакторах (то есть подделан). Таким образом, скриншот – всего лишь приложение к будущему протоколу осмотра, который не является сам по себе доказательством, а может являться таковым только в совокупности с остальными элементами протокола осмотра предмета[1].

Схожую точку зрения отстаивает и П.С. Пастухов, который справедливо указывает, что для эффективного противодействия преступлениям в сфере компьютерной информации следователю необходимо расширять как направления поиска, так и перечень предметов и документов – вещественных доказательств, в отношении которых следует осуществлять криминалистическую регистрацию. Поэтому целесообразно при расследовании преступлений делать акцент на фиксации и хранении следов сетевой активности пользователей, а также на взаимосвязи базовой станции и абонента[2].

Для этих целей следователь, начиная *рабочий этап* осмотра места происшествия, на основании судебного решения может получить информацию о соединениях между абонентами и (или) абонентскими устройствами. Ст. 186.1 УПК РФ, регламентирующая получение информации, имеет существенные ограничения для оперативного и всестороннего получения информации, а именно, одним из необходимых оснований для получения информации должно быть возбужденное уголовное дело по факту преступления, а информация должна предоставляться не в отношении лица, а в отношении конкретного абонентского номера (номеров). Стоит заметить, что для начала нужно установить владельца номера телефона, а также информацию о принадлежности пользователя провайдеру и его сетевой активности.

---

[1] Еськов В.Д., Чеботарев С.А. Особенности осмотра страниц в сети интернет // В сборнике: организационное, процессуальное и криминалистическое обеспечение уголовного производства Материалы VI Международной научной конференции студентов и магистрантов. – 2017. – С.39.

[2] Пастухов П.С. Правовые аспекты использования информационных технологий для обеспечения общественной безопасности и общественного порядка // Вестник Прикамского социального института. – 2016. – № 3(75). – С. 11.

Поэтому с целью предоставления расширенных результатов, помимо скриншота, следователь может дать поручение оперативному сотруднику провести ряд мероприятий, направленных на установление пользователя и компьютерного устройства, при помощи которого совершалась противоправная деятельность. Один из способов получения информации о компьютерном устройстве, (создание фишингового сайта), нами был рассмотрен в параграфе 3 главы 2-й. Обратим внимание, что некоторые интернет-ресурсы позволяют увидеть, при помощи какой операционной системы (Android, IOS, Windows) пользователь заходил на сайт, что дает представление о том, при помощи какого устройства он мог разместить информацию.

После выявления адреса устройства, при помощи которого совершалась противоправная деятельность, следующим этапом будет переход к фиксации его самого, при этом попутно также нужно установить точное время совершения деяния[1]. В некоторых судебных решениях с целью фиксации и использования компьютерной информации сотрудники правоохранительных органов составляли протокол, который подкрепляли скриншотами страниц пользователя в социальной сети «ВКонтакте», компакт-диском, содержащим записи с результатом осмотра страницы пользователя социальной сети «ВКонтакте», выпиской из федерального списка экстремистских материалов, получали заключение специалиста в области лингвистики[2]. Вместе с тем, в законодательстве отсутствуют четко зафиксированные требования, которые устанавливали бы, что именно должно прилагаться к протоколу. Так, например, при регистрации в социальной сети пользователь в открытом для просмотра доступе может оставить только фамилию и имя, что не дает 100 % оснований судить о принадлежности страницы конкретно этому лицу. В такой ситуации возникает необходимость проведения ряда тактических действий по установлению владельца сайта, где была опубликована информация, и осуществлению запроса у него информации касаемо действий пользователя на сайте. Обычно информация о владельце сайта указана во вкладке

[1] Карагодин В.Н., Костомаров К.В. Проблемы установления субъекта незаконного доступа к компьютерной информации банков // Библиотека криминалиста. Научный журнал. – М., 2013. – № 5(10). – С. 197.

[2] См.: Приложение № 2. Результаты анализа судебных решений.

«Контакты» или внизу сайта. В случае отсутствия такой информации на сайте за информацией о его владельце можно обратиться к операторам связи и интернет-провайдерам, если они предоставляли доступ в Глобальную сеть.

В анализируемой нами судебной практике можно заметить, что в некоторых случаях для подтверждения факта принадлежности страницы пользователю направлялся запрос к владельцу интернет-ресурса. В ответ на запрос предоставляется расширенная информацию о пользователе, а именно: полные анкетные данные пользователя, которые последний оставил при регистрации, а также e-mail, номер телефона, дата регистрации и IP-адрес, с которого проходила регистрация[1].

Приведем практический пример, где после установления владельца сайта ему был направлен запрос для получения дополнительной информации, а именно, на получение более развернутой информации касаемо имеющихся данных о подозреваемом пользователе. Данный пример наглядно отражен в постановлении Приморского районного суда г. Новороссийска (Краснодарский край) № 5-89/2017 от 18 января 2017 г. по делу № 5-89/2017, где говорится, что в отношении подозреваемого был сделан запрос в ООО «ВКонтакте» – по информации, представленной компанией ООО «ВКонтакте», пользователем «А» https://vk.com/id... является «ФИО» с регистрационными данными: e-mail, мобильный телефон, зарегистрирован в 2010 году с IP-адреса…[2].

По нашему мнению, полученных результатов может быть недостаточно, ведь при регистрации пользователь может указать анкетные данные, принадлежащие другому человеку или его страницу могут взломать, а с момента регистрации (2010 года, как указано выше в примере) IP-адрес может многократно измениться. Поэтому при составлении запроса стоит обратить внимание на такой раздел социальной сети «ВКонтакте» как «Защита данных», в котором говорится о возможности предоставления помимо адреса личной страницы пользователя,

[1] См.: Там же.

[2] Постановление Приморского районного суда г. Новороссийска (Краснодарский край) № 5-89/2017 от 18 января 2017 г. по делу № 5-89/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/oAodNVevI8Nh/ (дата обращения: 11.02.2025).

времени и IP-адреса, указанного на момент регистрации профиля, указывается также о возможности запросить историю смены имени пользователя и прикреплённого номера мобильного телефона, время и IP-адрес размещенного указанного в запросе контента, историю и перечень IP-адресов для входа на страницу. Целесообразным на данном этапе видится направить запрос провайдеру о подтверждении факта посещения сайта с IP-адреса, полученного в ответе от владельца сайта. Для полной картины стоит получить распечатку оператора сотовой связи, из которой станет известно месторасположение мобильного телефона, используемого подозреваемым, что подтвердит факт нахождения его на месте совершения преступления и принадлежности подозреваемому.

Однако, чтобы все проведенные действия признать доказательством и проверить их в условиях уголовного судопроизводства, необходимо последние процессуально закрепить. Это целесообразно сделать при помощи протокола осмотра предмета (документа). Здесь стоит остановиться на таком моменте, как исследование технического средства на наличие на нем материальных следов, а именно отпечатков пальцев рук, биологических следов, наличие повреждений. В такой ситуации Р.А. Дерюгин рекомендует перед изучением внутренней составляющей устройства тщательно произвести его внешний осмотр, надлежаще упаковать и назначить соответствующие экспертизы[1]. Мы считаем, что изучение компьютерной информации возможно начать сразу после обнаружения компьютерного устройства, для чего следует привлечь специалиста-криминалиста к выявлению и фиксации материальных следов на месте.

Казалось бы, теперь следователь, заведомо зная о принадлежности компьютерного устройство подозреваемому и нахождении на нем информации, имеющей значение в расследовании, может приступить к заключительному этапу, а именно, проводить осмотр предметов с целью надлежащей фиксации и получения из устройства информации. Информация, находящаяся на осматриваемом устройстве должна быть сохранена на внешних носителях, к примеру, с помощью

[1] Дерюгин Р.А. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия и использование его результатов при расследовании преступлений: дис. ... канд. юрид. наук: 12.00.12 / Дерюгин Роман Александрович. – Екатеринбург, 2018. – С. 138.

такой программы как «Мобильный криминалист», программно-аппаратного комплекса UFED[1].

Однако, анализируя действующее законодательство и правоприменительную практику, М.С. Садырова и М.М. Менжега не согласны с тем, что извлечение информации, например, из мобильных устройств может осуществляться в рамках такого следственного действия, как осмотр предметов. Авторы отмечают, что сведения в мобильном устройстве не подпадают под признаки предмета, следовательно, изъять их в ходе обыска или, например, выемки не представляется возможным, в силу чего следственное действие «осмотр предмета» связано только со сбором доказательств путем внешней проверки его конструкции, выявления индивидуальных черт, отличительных признаков от идентичных предметов и т. д.[2]. О том, что осмотр полностью исключает процесс исследования телефона также указывают Д.К. Воронкова и А.К. Манучарян[3].

Получается, что следственные действия ограничиваются в оперативном получении компьютерной информации в отношении подозреваемого лица. Поэтому тактическим приемом на этапе осмотра будет поручение сотрудникам оперативных подразделений, используя, в частности, ОРМ «Получение компьютерной информации», получение и фиксацию соответствующей доказательственной информации. Например, при осмотре мобильных телефонов оперативные сотрудники неоднократно обнаруживали информацию, указывающую на признаки противоправной деятельности:

- в установленном программном обеспечении (мессенджерах «Telegram»[4], «WhatsApp»[5] и т. д.);

---

[1] Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук: 5.1.4 / Харина Елена Алексеевна. – Красноярск – 2024. – С.179.

[2] Садырова М.С., Менжега М.М. Осмотр электронных устройств как самостоятельное следственное действие // Юридические науки: проблемы и перспективы: материалы IV Междунар. науч. конф. – Казань: Изд-во «Бук», 2016. – С.279.

[3] Воронкова Д.К., Манучарян А.К. Осмотр и судебная экспертиза мобильного устройства в рамках расследований по уголовным делам // Международный журнал гуманитарных и естественных наук. – 2019. № 7-2. – С.119.

[4] Приговор Лесосибирского городского суда (Красноярский край) № 1-275/2018 от 18 октября 2018 г. по делу № 1-275/2018 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/YXnsYURSnoJL/ (дата обращения: 09.02.2025).

[5] Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-164/2017 от 18 августа 2017 г. по делу № 1-164/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TweV9tbuut5Z/ (дата обращения: 09.02.2025).

- в папке «Галерея» (видео и фотографии)[1];

- в папке «Диктофон» (аудиозаписи)[2] и т. д.

В большинстве случаев как доступ к программному обеспечению, так и к компьютерному устройству правонарушителя может быть закрыт пользователем парольной защитой и поэтому следователь может принять решение об изъятии мобильного телефона и направлении его на судебную компьютерно-техническую экспертизу. Однако практика судебных дел показывает, что эта проблема успешно разрешается сотрудниками оперативных подразделений на месте. В частности, из справки по результатам проведения ОРМ «Получение компьютерной информации», которая зафиксирована в приговоре Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-244/2017 от 17 ноября 2017 г. по делу № 1-244/2017, видно, что у подозреваемого был изъят мобильный телефон, который мог содержать оперативно-значимую информацию для расследования преступления. При помощи мобильного телефона был осуществлен вход на сайт, при этом в поле «имя» и «пароль» были внесены полученные от подозреваемого данные, после чего была получена компьютерная информация с его личного кабинета[3].

Не лишним будет указать, что сотрудники оперативных подразделений в рамках ОРМ «Получение компьютерной информации» с целью фиксации компьютерной информации могут использовать различные технические средства, в том числе и личные. Здесь стоит привести как пример приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-322/2017 от 9 ноября 2017 г. по делу № 1-322/2017, где говорится о том, что оперативному сотруднику с целью получения компьютерной информации оперативного значения поступило указание от начальника и в дальнейшем получено от него постановление провести

[1] Приговор Приморского районного суда г. Новороссийска (Краснодарский край) № 1-458/2017 1-63/2018 от 2 февраля 2018 г. по делу № 1-458/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/gaRcTHh7C6dC/ (дата обращения: 09.02.2025).

[2] Приговор Приморского районного суда г. Новороссийска (Краснодарский край) № 1-130/2017 от 17 мая 2017 г. по делу № 1-130/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/GPSNpiTKsHYB/ (дата обращения: 09.02.2025).

[3] Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-244/2017 от 17 ноября 2017 г. по делу № 1-244/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/QODcLxpWm5dr/ (дата обращения: 10.02.2025).

ОРМ «Получение компьютерной информации» из мобильного телефона, принадлежащего гр. «К». Сотрудник полиции перед проведением ОРМ получил у гр. «К» добровольное согласие на осмотр его мобильного телефона. В присутствии понятых телефон был исследован. В телефоне были найдены описания местонахождения закладок с наркотическими веществами. Для этого мобильный телефон был подключен к компьютеру, который находился в пользовании оперативного сотрудника, куда были скопированы и в последствии распечатаны скриншоты с результатами ОРМ «Получение компьютерной информации»[1].

Вместе с тем, проведение вышеуказанного ОРМ иногда все же может приводить к нарушению конституционных гарантий права на частную жизнь (ст. 23 Конституции РФ), а именно на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения[2].

В правоохранительной практике встречаются противоположные примеры – когда в одном случае суд не усматривает нарушения данных конституционных гарантий правоохранителями, в других случаях такие гарантии признаются нарушенными. Из проанализированной нами судебной практики видно, что из 60 случаев при проведении ОРМ только в 5-ти обращались в суд за разрешением[3].

В ходе опроса оперативные сотрудники указали, что в 97% случаях подозреваемый дает добровольное согласие на получение доступа к его компьютерной информации[4] и, соответственно, решения суда не требуется.

Когда пользователь, например, отказывается предоставить пароль для доступа к принадлежащему ему устройству, сотрудник ОВД может самостоятельно обойти защиту. Показательным здесь является способ, отраженный в приговоре Фрунзенского районного суда г. Владимира (Владимирская область, Российская Федерация) за № 1-86/2018 от 24 сентября 2018 г. по делу № 1-86/2018, сущность

---

[1] Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-322/2017 от 9 ноября 2017 г. по делу № 1-322/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/5RIILb1PXPUz/ (дата обращения: 08.02.2025).

[2] Конституция Российской Федерации от 12 декабря 1993 года [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[3] См.: Приложение № 2. Результаты анализа судебных решений.

[4] См.: Приложение № 1. Опросный лист.

которого заключается в следующем.

Возникла ситуация, когда подозреваемый отказался предоставить пароль от своего телефона, однако оперативный сотрудник, зная способ получения (восстановления) пароля, с целью получения переписки, содержащейся на телефоне, изъятом при личном досмотре подозреваемого в присутствии двух понятых, попросил подозреваемого сообщить свой номер телефона, который впоследствии сотрудник внес в свой телефон в приложении «Telegram», и самостоятельно получил пароль. Благодаря такому способу была получена переписка с пользователем, причастным к совершению преступления[1].

Считаем, что в данной ситуации оперативный сотрудник действовал в рамках предписаний п. 8 ст. 8 ФЗ «Об оперативно-розыскной деятельности», в котором указано, что без судебного решения разрешается проводить ОРМ на основании мотивированного постановления руководителя органа, осуществляющего ОРД. В указанном примере такое постановление от вышестоящего руководителя было получено, после чего в течение 48 часов было получено также судебное разрешение на проведение указанного ОРМ.

Интересное мнение высказывает В.Ф. Васюков, который, рассматривая необходимость получения судебного решения на проведение ОРМ, связанных с получением компьютерной информации, указывает на то, что, если информация выбыла из сферы ответственности организации (должностного лица) путем фиксации ее, например, в памяти мобильного компьютерного устройства, она как таковая уже не подлежит защите с помощью судебного контроля[2].

Так, с целью эффективного использования компьютерной информации в уголовном производстве, следователь должен произвести не изучение информации, находящийся на электронном носителе, а осмотреть само устройство (предмет) и зафиксировать его индивидуальные признаки и особенности. Для придания зафиксированной компьютерной информации доказательственного

---

[1] Приговор Фрунзенского районного суда г. Владимира, Владимирская область, Российской Федерации. - № 1-86/2018 от 24 сентября 2018 г. по делу № 1-86/2018 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TqnXFydxjZx4/ (дата обращения: 10.02.2025).

[2] Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. – 2016. – № 10. – С. 67.

значения на *заключительным этапе* должно стать оформление полученной оперативным сотрудником информации протоколом осмотра предмета (документа).

Допрос. В целях всестороннего и полного исследования обстоятельств противоправной деятельности, осуществляемой при помощи компьютерных устройств, нужно не только выявить факт и произвести фиксацию его совершения, но также получить сведения от лица, его совершившего. Для этого необходимо допросить как лицо, причастное к такой деятельности, так и тех, кто может располагать информацией о совершенном противоправном деянии. Убедительным здесь видится высказывание А.И. Просиной в отношении того, что допрос можно определить как следственное действие, в котором познаётся вся суть совершаемого преступления[1]. Именно при допросе происходит личное общение следователя с допрашиваемым, где наличие четких тактических приемов дает гарантию получить ценную и исчерпывающую информацию об обстоятельствах, подлежащих доказыванию по уголовному делу.

В этой связи стоит также выделить некоторые тактические особенности использования компьютерной информации, а именно: предоставление имеющейся у следователя компьютерной информации в ходе допроса.

Очевидно, что для достижения максимального результата в кратчайшие сроки особую ценность приобретает *подготовительный этап.* В процессе подготовки следователя к допросу, помимо изучения сведений, полученных от ранее опрашиваемых лиц по делу, целесообразно выявить как можно больше компьютерной информации о допрашиваемых. Изучение личности допрашиваемого помогает следователю определиться с особенностями процесса формирования показаний и выработать нужную тактику допроса.

Изучение личности допрашиваемого в тех случаях, когда это необходимо, следует начать сразу же, как только принимается решение о его допросе. И здесь необходимо остановиться на данных, которые могут быть получены в ходе

[1] Просина А.И. Соблюдение статьи 51 Конституции Российской Федерации при проведении допроса: история и современность // Наука. Общество. Государство, 2018. – №. 4 (24). – С. 5.

проведения ОРМ.

На подготовительном этапе к допросу результаты ОРМ могут способствовать выяснению обстоятельств совершения преступления, которые касаются:

- навыков и опыта работы с компьютерной техникой и конкретным программным обеспечением;

- каким компьютерным устройством и программным обеспечением пользуется допрашиваемый, при помощи какого интернет-провайдера или оператора связи пользователь осуществляет подключение к Интернету, какие интернет-ресурсы посещает и какие при этом интернет-сервисы использованы для регистрации;

- какие действия допрашиваемый производит в компьютерной сети, а именно, с кем, в какое время и при помощи каких интернет-ресурсов и компьютерных устройств ведет переписку, где и когда была получена и каким способом размещена компьютерная информацию противоправного характера, кому такая информация была отправлена, а также кто ещё ею мог воспользоваться.

Также, на практике возникают ситуации, когда после нахождения в открытых источниках компьютерной информации, которая может представлять интерес для расследования, но не может быть проверена гласными способами, есть смысл дать поручение оперативному сотруднику перепроверить данную информацию и впоследствии отследить источник ее опубликования.

Тактическим приемом будет проверка достоверности полученной информации путем общения сотрудника ОВД с пользователями на сайте, тем самым не только можно удостовериться в ее актуальности, но и узнать дополнительные детали касаемо проверяемой информации и лица, который ее разместил, например, сленговые выражения, его общественное настроение, адрес электронной почты и т. д.

На подготовительном этапе следователь также должен подготовить и, по возможности, процессуально оформить имеющуюся у него компьютерную информацию (скриншоты, справки от владельца интернет-ресурса, интернет-провайдера, оператора связи).

Рабочий этап стоит начать с предоставления в процессе допроса скриншотов страниц пользователя с перепиской или с размещенной им в сети Интернет информацией противоправного характера. По мнению отдельных авторов, убедившись в том, что, если осуществлена фиксация противоправных действий при помощи информационных технологий и в последующем такая информация может быть представлена суду, злоумышленники во многих случаях предпочитают чистосердечное признание, рассчитывая на смягчение наказания при рассмотрении дела в ходе судебного заседания.[1]

Однако здесь необходимо обратить внимание на тот факт, что лицо может и отрицать принадлежность компьютерной информации конкретно ему, обосновывая это тем, что его компьютерным устройством мог пользоваться другой человек. В данном случае следователю стоит поинтересоваться, с какого момента компьютерным устройством пользовался подозреваемый и используя данные, полученные ранее от оператора связи, сравнить с теми, когда было совершено преступление.

При рабочем этапе допроса имеет значение выяснение обстоятельств, которые предшествовали совершению преступления:

- когда возникло намерение совершить преступление, кто или что повлияло на это решение;

- почему выбран тот или иной объект для преступного посягательства;

- каковы мотивы совершения преступления (подавляющее большинство - более 70% - совершаются по корыстным мотивам)[2].

Следователь в ходе допроса может использовать следующую информацию:

- о конкретных преступных действиях допрашиваемого, а также мотивах и целях;

- о его связях, о взаимоотношениях с другими пользователями, а также его месте и роли в преступном сообществе. Такие данные можно получить из

---

[1] Кузнецов А.А., Муленков Д.В. Тактические и технические аспекты работы с цифровыми средствами фиксации при проведении оперативно-розыскных мероприятий // Юридическая наука и правоохранительная практика, - 2009. – №. 1 (7). – С.48.

[2] Домашенко И.Е. Тактика подготовительной части допроса по преступлениям в сфере компьютерной информации // Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования. – 2015. – С. 3074.

социальных сетей путем просмотра раздела «Друзья» или из форумов, блогов, сообществ(групп), а также иных интернет-ресурсов, где пользователь осуществлял свою противоправную деятельность и вел переписку и (или) был запечатлен на фотографиях;

- о личности допрашиваемого, а именно, возрасте, семейном положении, образовании, жизненной позиции, увлечениях и всей той информации, которая указана в его профиле;

- о действиях иных лиц, оказывающих помощь в подготовке и сокрытии преступления или иной сопутствующей этому информации. Такие сведения могут быть отражены в группах, на которые пользователь подписан в социальных сетях, или в новостях, которые допрашиваемый просматривал и оставлял свои комментарии;

- о часто употребляемых словах в комментариях и о времени посещения интернет-ресурсов.

Использовать такую информацию при допросе можно по-разному: учитывая ее при определении очередности вопросов и их формулировке, для достижения превосходства, для восполнения картины события при демонстрации осведомленности о деталях преступления и роли в его совершении допрашиваемого[1].

Не смотря на тот факт, что первичное обнаружение незаконных действий при помощи компьютерной информации осуществляется силами и средствами оперативных сотрудников, описание признаков этих действий можно также найти и в свидетельствах очевидцев.

При этом необходимо учитывать, что свидетелями по данной категории дел часто являются лица, употребляющие особую терминологию, которая не всегда понятна следователю. В связи с этим необходимо получить более подробные сведения от допрашиваемых, задавая уточняющие вопросы, раскрывающие содержание используемых ими терминов и определений.

Кроме этого, содержание самого механизма преступного деяния таково, что

[1] Криминалистика: учебник для вузов / Под ред. Р.С. Белкина. – М.: НОРМА, 2001. – С. 601-602.

при выяснении всех его элементов и обстоятельств совершения требуется наличие знаний о: виртуальной сфере, в которой совершаются подобного рода преступления; специфике компьютерной информации. Эти знания зависят от применяемых для реализации преступного умысла орудий и средств – компьютеров, накопителей информации, компьютерных сетей и доступа к ним и др. В этой связи наиболее актуальными являются вопросы привлечения специалиста к участию в таком следственном действии, как допрос[1].

Для участия в допросе следователь может пригласить в качестве специалиста не только лицо, обладающее углубленными знаниями в области вычислительной техники, но также субъектов, которые активно посещают и давно являются пользователями ресурса, представляющего интерес для следствия. Такие субъекты могут обладать знаниями, например, о функционировании определенной программы или значении некоторых сленговых выражений, которые могут употребляться только на конкретном ресурсе. В ходе беседы со специалистом может выясниться, что он установил личность подозреваемого лица, например, по его логину или по его выражениям, на основании чего может ставиться вопрос о привлечении такого специалиста в качестве свидетеля по делу.

Если осуществлялись дополнительные ОРМ, то полученные в ходе них данные могут быть введены в процесс путем допроса соответствующего лица в качестве свидетеля. Например, если использовались технические средства, предусмотренные ч. 3 ст. 6 ФЗ «Об оперативно-розыскной деятельности», то полученные материалы могут использоваться при проверке и оценке показаний допрашиваемых по делу участников[2].

На *заключительном этапе* допроса в случае, если имеются сведения об использовании компьютерной информации в процессе совершения преступлений или если есть данные, подтверждающие противоправную деятельность лица, то

[1] Смирнова И.Г., Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Baikal Research Journal. 2015. vol. 6, №. 3. – URL: http://brj-bguep.ru/ (дата обращения: 07.02.2025).

[2] Колесников А.В. Использование результатов оперативно-розыскной деятельности при выявлении и расследовании преступлений против личности // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2016. – № 1. – С. 86.

следователь должен не только зафиксировать имеющиеся данные об использовании компьютерной информации, но и указать в протоколе все возможные источники и ресурсы, где пользователь мог обмениваться или получать информацию.

Обобщая изложенное, в заключении необходимо отметить, что возможности компьютерных технологий, в отличии от традиционных способов, позволяют более детально зафиксировать компьютерную информацию при помощи ОРМ и следственных действий и в последствии превратить ее в доказательства. Однако для придания таким результатам процессуальной формы и использования их в качестве доказательства, необходимо фиксировать не только факт совершения противоправного действия, но также провести всестороннее исследование дополнительной информации, что может способствовать успешному проведению таких отдельных следственных действий, как осмотр предмета (документа), допрос подозреваемого, свидетелей и оперативных сотрудников.

Следователь во время проведения следственных действий может давать поручения оперативному сотруднику по поводу проведения дополнительных мероприятий, направленных на установление времени посещения пользователем различных ресурсов сети Интернет, его связей, интересов, комментариев на форумах и блогах, а также поручения по поводу направления запросов владельцам интернет-ресурсов, операторам мобильной связи и интернет-провайдерам на предмет установления сетевой активности пользователя и о принадлежности ему оборудования. Полученные в ходе ОРМ результаты могут являться ориентиром для установления пользователя (ФИО, IP-адрес, e-mail, номер мобильного телефона) и предмета, 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, содержащего сведения о противоправной деятельности, а в случае отрицания принадлежности информации подозреваемому,

предъявление справки об активности пользователя от оператора связи, интернет- и хостинг- провайдера, владельца интернет-ресурса, что может указывать не только на осведомленность об обстоятельствах, имеющих отношение к расследуемому событию, но также и на то, что эта информация уже закреплена как доказательство.

§ 3.3. Особенности использования современных информационных технологий в практике расследования преступлений

Получение, фиксацию и дальнейшее использование компьютерной информации при противодействии преступлениям в настоящее время сложно представить без интеграции в деятельность ОВД информационных технологий, а также, как обосновано отмечают отдельные ученые, без разработки действенных механизмов реализации сопутствующих правовых норм[1].

Здесь также уместно высказывание И.Ю. Антонова, по мнению которого технические средства – важнейший инструмент деятельности по выявлению, раскрытию и расследованию преступлений. Без современных информационных технологий сегодня невозможно представить проведение и фиксацию результатов большей части оперативно-розыскных мероприятий[2]. Очевидно, что развитие информационных технологий и внедрение их достижений в расследование, способны значительно помочь, в том числе, и следователю в его работе[3].

Возникает необходимость постоянного усовершенствования компьютеризации процесса расследования преступлений, внедрения искусственного интеллекта, что даст возможность в полном объеме обеспечить сотрудника ОВД информацией высокого качества и в максимально короткое время реализовать пополнение этой информации в ходе расследования из различных

---

[1] Швец С.В. Криминалистическая тактика следственных и судебных действий в условиях использования перевода: автореф. д-ра юрид. наук / С.В. Швец. – Краснодар, 2014. – С. 20.

[2] Антонов И.Ю. Некоторые направления совершенствования оперативно-розыскного мероприятия «Наблюдение», проводимого с применением технических средств // Общество и право. – 2015. – № 2(52). – С. 217.

[3] Грицаев С.И., Помазанов В.В., Заболотняя Ю.А. Компьютеризация целеопределения и планирования расследования // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2015. – № 108. [Электронный ресурс]. – URL: http://ej.kubagro.ru/2015/04/pdf/36.pdf (дата обращения: 25.01.2025).

источников[1].

Но, прежде чем рассматривать компьютеризацию в ОВД РФ, есть смысл упомянуть, что первоначально получением компьютерных данных начали заниматься спецслужбы США, когда в 90-х годах появились первые упоминания о деятельности глобальной системы радиоэлектронной разведки «Эшелон», основной целью которой стал перехват данных на международном уровне. Впрочем, в виду актуальности системы, «Эшелон» остается глубоко засекреченной системой и все сведения о нем не совсем достоверны.

Одновременно с вышеуказанной системой «Эшелон», в конце 90-х годов прошлого века, в США была запущена в эксплуатацию внутригосударственная система обеспечения оперативно-розыскных мероприятий, проводимых в сети Интернет. Она получила кодовое название «Плотоядное животное» («Carnivore»), которое в последующем было заменено на менее вызывающее «DCS-1000».

Эта система позволяет правоохранительным органам осуществлять мониторинг электронной почты и ftp-трафика[2].

Официальной, отправной датой создания систем, направленных на получение компьютерной информации в США, является 11 сентября 2001 года. Именно после этого события Федеральное бюро расследований (далее-ФБР) усилило электронное наблюдение в компьютерной сети.

Поскольку террористы также пользуются обычной электронной почтой, спецслужбам США еще до совершения теракта 11 сентября было известно о его подготовке. Уже через короткое время после трагедии агенты ФБР начали активный поиск исполнителей. С этой целью провайдерским компаниям было предложено установить специальное программное обеспечение на их почтовых серверах для перехвата электронной почты – DCS-1000, позволяющее сканировать весь почтовый трафик и выявлять подозрительные имена и словосочетания.

В настоящее время помимо получения компьютерной информации,

---

[1] Корчагин А.А., Кобзев И.В. Информационно-программное обеспечение доследственных, следственных и судебных ситуаций по уголовным делам об убийствах // Известия АлтГУ. – 2015. – № 2(86). – С. 75.

[2] Лоскутов И.Ю. Сравнительный анализ международных норм законодательного регулирования Интернета в различных странах (2008 год) [Электронный ресурс]. – URL: http://www.zakon.kz/221107-sravnitelnyjj-analiz-mezhdunarodnykh.html (дата обращения: 28.01.2025).

внимание уделяется и ее защите (блокированию). Так, в некоторых государствах, в том числе и РФ, это направление считается приоритетной задачей в сфере национальной безопасности и международной политики. При этом концепция информационной безопасности включает как защиту пользователей сетей, так и защиту государства и его критических инфраструктур[1], что достигается путем просмотра и блокирования компьютерной информации.

Параллельно с системой перехвата создавались инструменты для фильтрации и мониторинга сети Интернет. Одна из них создана в Китае и известна под общим названием «Великий брандмауэр Китая» (Great Firewall). Помимо обычных правил маршрутизации, которые позволяют заблокировать доступ к IP-адресу или конкретному доменному имени, Great Firewall широко использует технологию Deep Packet Inspection (далее – DPI) для мониторинга и блокировки доступа на основе обнаружения ключевых слов. У Great Firewall есть возможность динамически блокировать зашифрованные соединения. Один из основных интернет-провайдеров страны, China Unicom, автоматически отключает соединение, как только оно используется для передачи зашифрованного контента[2].

Система мониторинга, разработанная Китаем, не ограничивается Great Firewall, мониторинг также встроен в социальные сети, чаты, VoIP и даже в приложение для мгновенного обмена сообщениями, например, такие, как QQ, что позволяет властям страны подробно отслеживать обмен информацией между пользователями Интернет, путем поиска определенных ключевых слов и выражений. Автор каждого сообщения может быть идентифицирован номером пользователя. Приложение QQ – это действительно гигантский троянский конь. А с марта 2012 года китайское законодательство требует, чтобы все новые пользователи сайтов с микро-блогом регистрировались с использованием своего имени и номера телефона.

Рассматривая вышеуказанные системы, стоит понимать, что их работа

---

[1] Журавленко Н.И., Шведова Л.Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. – 2015. – № 3(53). – С. 70.

[2] Mass surveillance [Электронный ресурс]. – URL: https://www.revolvy.com/topic/Mass%20surveillance&item_type=topic (дата обращения: 06.02.2025).

основана на перехвате и фиксации правоохранительными органами передаваемой компьютерной информации, осуществляемой через операторов связи, предоставляющих услуги доступа к компьютерной сети.

В России способом получения оперативно-значимой информации на сетях связи является использование имущества операторов связи (третьих лиц). Частью 4 ст. 15 ФЗ «О Федеральной службе безопасности»[1] предусмотрено, что «физические и юридические лица в Российской Федерации, предоставляющие услуги ... электросвязи всех видов, ... обязаны ... включать в состав аппаратных средств дополнительное оборудование и программные средства, а также создавать другие условия, необходимые для проведения оперативно-технических мероприятий органами ФСБ»[2]. Во исполнение пункта 2 статьи 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» и пунктов 4, 6, 11 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденных постановлением Правительства Российской Федерации от 27 августа 2005 г. № 538, были закреплены требования к сетям электросвязи, где сказано, что на последних должны устанавливаться технические средства для проведения оперативно-розыскных мероприятий (далее – СОРМ)[3].

Благодаря СОРМ стало возможным получить доступ к компьютерной информации, передаваемой в соединении и (или) сообщении электросвязи абонентов, информации о местоположении абонентов, в отношении которых принято решение о проведении оперативно-розыскных мероприятий, устанавливать постоянный IP-адрес, IP-адрес, определяемый по маске, имя учетной записи пользователя, используемое для идентификации пользователя

[1] О Федеральной службе безопасности: Федеральный закон от 03 апреля 1995 № 40-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

[2] Немкова Н.А. Особенности правового регулирования оперативно-розыскных мероприятий в сетях связи // Проблемы правоохранительной деятельности. – 2009. – № 1-2. – С. 70.

[3] Об утверждении Требований к сетям электросвязи для проведения оперативно-разыскных мероприятий: Приказ Министерства информационных технологий и связи Российской Федерации от 16 января 2008 г. – № 6 [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102094659&backlink=1&&nd=102120563 (дата обращения: 12.02.2025).

услуг связи при доступе к сети передачи данных и телематическим услугам связи, электронный почтовый адрес сервисов Web-mail, использующих средства защиты информации, включая криптографические, телефонный номер пользователя (вызываемого и (или) вызывающего), идентификатор абонентской телефонной линии, используемый для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи, идентификатор вызываемого и вызывающего пользователя услуг связи по передаче данных для целей передачи голосовой информации, международный идентификатор абонента сети подвижной связи (IMSI), международный идентификатор мобильного оборудования (IMEI), уникальный идентификатор оборудования сетей передачи данных (MAC-адрес), идентификатор служб обмена сообщениями (включая ICQ), мобильный идентификационный номер мобильной абонентской радиостанции (MIN) и др.[1].

Придание огласке информации, что сотрудники ФСБ при помощи СОРМ смогут следить за интернет-пространством, вызвало широкое обсуждение среди пользователей сети, мнения которых разделились, являясь диаметрально противоположными. С одной стороны, если человеку нечего скрывать, то ему и нечего бояться. Поэтому такой шаг действительно необходим. С другой стороны, как отметило в своем письме, направленном в Минкомсвязи ОАО «Вымпел-Коммуникации», подобные действия противоречат Конституции Российской Федерации в части прав и свобод частной жизни граждан. Операторы связи заявили о том, что некоторые нормативные положения предполагают сбор и хранение данных до решения суда (все интернет-провайдеры будут обязаны установить на свои сети оборудование для записи и хранения интернет-трафика на срок не менее 12 часов, причем спецслужбы получат к ним прямой доступ)[2]. Необходимо отметить, что деятельность, связанная с получением компьютерной информация при помощи СОРМ, доступна только сотрудникам ФСБ[3].

---

[1] Батоев В.Б. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет // Вестник ВИ МВД России. – 2016. – № 2. – С. 39-40.

[2] Ковалев С.И., Иванская А.В. Проблемы правовой защиты информации приватного характера в условиях развития научно-технического прогресса // Вестник РУДН. Серия: Юридические науки. – 2014. – № 1. – С. 47.

[3] Страшный и ужасный СОРМ2: немного практики [Электронный ресурс]. – URL:

Обоснованно возникает вопрос о возможности получения при помощи СОРМ компьютерной информации не только сотрудниками ФСБ, но и другими оперативными подразделениями. Ведь в ст. 64 ФЗ «О связи» указано, что субъекты, которые предоставляют доступ к компьютерной информации и впоследствии обязаны хранить 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 и должны 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[1]. То есть, лица, оказывающие услуги связи на основании лицензии (операторы связи), должны предоставлять всем оперативным подразделениям компьютерную информацию на равных условиях. Стоит акцентировать внимание на том, что, имея доступ к СОРМ, субъекту оперативно-розыскной деятельности в режиме реального времени предоставляется дополнительная возможность получать информацию об истории нахождения человека в различных интернет-ресурсах.

Ключевым моментом является тот факт, что информация, передаваемая по каналам связи при помощи программного обеспечения, с целью сокрытия от неавторизированных лиц подвергается различного рода шифрованию, что, в свою очередь, также вызывает затруднения при доступе к последней оперативных сотрудников.

Для решения этих задач активно обсуждается набор технических решений, которые позволят реализовать дешифровку и, соответственно, полный доступ к информационному потоку Российского сегмента сети Интернет.

Как один из вариантов его дешифровки и анализа рассматривается применение систем DPI, используемых в данный момент провайдерами для

---

https://habr.com/ru/post/65924/ (дата обращения: 13.02.2025).

[1] О связи: Федеральный закон от 07 июля 2003 № 126-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.01.2025).

фильтрации и блокировки запрещенного контента. Так, на данный момент на законодательном уровне хранить интернет-трафик операторов уже обязывает «закон Яровой», но сам по себе без дешифровки он бесполезен. При помощи технологии DPI возможно проверять содержимое информационных потоков и на основе этого определить адрес, номер порта и используемого протокола. Несмотря на довольно высокую эффективность данного подхода в блокировке нежелательного контента полную расшифровку содержимого информационного потока он не позволяет сделать. Кроме того, оборудование для DPI сложно настраивать, и оно к тому же дорого стоит.

Также обсуждаемые подходы полной дешифровки личных данных несут в себе целый ряд опасностей в части нарушения таких прав человека, как право на неприкосновенность частной жизни и право на тайну переписки. По мнению экспертов, в конечном итоге полная дешифровка позволит не только предотвращать потенциальные угрозы, но и строить профили поведения граждан – вплоть до оценки их психологического состояния, предпочтений и других личных данных[1].

Принципиально обеспечить полную анонимность в сети Интернет нельзя. Как нам известно, любые сетевые взаимодействия оставляют следы. Однако затруднить привязку абонента (технического средства) к информации, выложенной в Интернете, можно. Наиболее эффективно делается это с помощью средств Невидимого Интернета – анонимных сетей. Здесь возникает проблема, связанная с установлением конечного оборудования, а именно, при помощи которого пользователь запрашивает (передает) информацию через анонимные сети.

На данный момент для установления компьютерной информации, свидетельствующей о противоправной деятельности в анонимных сетях, уже сделаны некоторые шаги. Так, с целью поиска и выявления места подключения личностей (или организаций), которые организовали подключения, такую задачу возможно реализовать путем фильтрации интернет-трафика. В процессе

[1] Шифр и меч, ФСБ собирается взять интернет-трафик на контроль [Электронный ресурс] «Коммерсант». – URL: http://kommersant.ru/doc/3094848 (дата обращения: 22.01.2025).

фильтрации необходимо сделать сортировку тех пользователей, которые пытаются подключаться к сетям анонимно. Каждое анонимное подключение должно фиксироваться в автоматическом режиме, параллельно должна происходить запись, в какое время и каким образом пользователь осуществлял подключение. Однако, в РФ такие действия не позволяют в полной мере реализовать механизм автоматической деанонимизации людей и организаций, стоящих за такими подключениями. Но, по всей видимости, эта проблема уже решена в АНБ США относительно некоторых анонимных сетей, таких, например, как Tor.

В России 16 марта 2019 года был принят ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»». Данными нормативно-правовыми актами предусмотрена возможность осуществления блокирования пока лишь подозрительных и анонимных интернет-ресурсов, начиная от сайтов из единого реестра и фейковых новостей, Telegram и нелояльных VPN-провайдеров[1]. Считаем, что для правоохранительных органов России указанного законодательного шага недостаточно. Так, например, в 2014 году МВД России объявило тендер на исследование возможности деанонимизировать всех пользователей Tor[2], что, конечно же следовало реализовать.

Министерством внутренних дел РФ проводятся тендеры на проведение исследований и поставку оборудования, используемого для выявления анонимных пользователей сети Интернет и дальнейшего препятствования их противоправной деятельности. Для деанонимизации было выделено порядка 34 млн. рублей, косвенно – еще как минимум 35 млн. рублей. Наибольший интерес здесь может представлять конкурс, касающийся Tor – системы прокси-серверов, позволяющей устанавливать анонимное сетевое соединение, теоретически защищенное от прослушивания. В числе прочих задач эта система используется для

[1] О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» Федеральный закон Российской Федерации от 01 мая 2019 № 90-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

[2] Куватов В.И., Примакин А.И., Якушев Д.И. Противодействие террористическим и экстремистским организациям в сети Интернет // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 1(65). – С. 93.

распространения контента, передача которого может быть законодательно запрещена в той или иной стране[1].

На следующий день после публикации материала об этих конкурсах в издании CNews большая часть названий тендеров, по которым можно было хотя бы приблизительно судить о содержательной части предстоящих работ, была сокращена до внутриведомственных шифров.

Так, например, до 24 июля 2014 г. один из конкурсов именовался «Выполнение ОКР «Создание аппаратно-программного комплекса по проведению негласного и скрытого удаленного доступа к оперативно-значимой информации на целевой электронно-вычислительной машине», шифр «Хамелеон-2 (Флот)»». С утра 25 июля он называется просто «Выполнение опытно-конструкторской работы, шифр «Хамелеон-2 (Флот)»».[2] Такое решение в дальнейшем не было реализовано на практике. Поэтому считаем, что повышение эффективности в деле противодействия киберугрозам должно быть достигнуто за счет максимального снижения степени анонимности личности при использовании интернет-сетей общего доступа. С этой целью нами было предложено разработать, нормативно закрепить и в последующем внедрить в правоохранительную практику соответствующий программно-аппаратный комплекс идентификации интернет-пользователей. Физическая идентификация личности должна происходить в специальных удостоверяющих центрах, где пользователь сети Интернет перед тем, как использовать компьютер, программное обеспечение и компьютерные сети, обязан будет получать уникальный криптографический ключ-идентификатор (далее – идентификатор). С другой стороны, нужно сделать так, чтобы программно-аппаратный комплекс идентификации совместно с криптографическим ключом предоставлял возможность фиксировать действия пользователя при работе с компьютером, программным обеспечением и компьютерной сетью на всех уровнях

[1] Информационный ресурс «cnews.ru» МВД потратит 70 млн руб., чтобы уничтожить приватность в Рунете [Электронный ресурс]. – URL: http://www.cnews.ru/news/top/mvd_potratit_70_mln_rub.chtoby_unichtozhit (дата обращения: 22.01.2025).

[2] Информационный ресурс «cnews.ru» МВД строит Единую информационно-аналитическую систему за 1,5 млрд руб. [Электронный ресурс]. – URL: http://www.cnews.ru/news/top/mvd_stroit_edinuyu_informatsionnoanaliticheskuyu (дата обращения: 22.01.2025).

их взаимодействия. Иными словами, для пользователя возможность воспользоваться услугами интернет-провайдера или осуществить регистрацию на сайте будет ограничена до тех пор, пока им не будет использован личный идентификатор[1].

Актуальным остается высказывание Р.Н. Вязовец, который указывал, что использование информационных технологий в ОВД РФ преимущественно сводится к созданию государственных информационно-справочных систем или, как еще их принято называть, Банков данных[2]. Основной задачей Банков данных в органах внутренних дел является оперативное предоставление накопленной компьютерной информации при расследовании и раскрытии преступлений.

Несмотря на тот факт, что компьютерную информацию, представляющую интерес при раскрытии и расследовании преступлений, сотрудник ОВД может получать из различных информационных источников, однако первоочередными и наиболее актуальными являются информационные системы, функционирующие и активно разрабатываемые в МВД.

Получение, изменение и добавление информации в Банки данных ОВД может осуществляться глобально и охватывать все регионы государства.

Уже сейчас результативность работы правоохранительных органов по предупреждению, раскрытию и расследованию преступлений невозможна без своевременного, достаточного и качественного информационного обеспечения, считает Р.Е. Демина. Упреждающая информация может быть получена, в основном, путем использования методов и возможностей оперативно-розыскной деятельности при условии рационального сочетания технико-криминалистических средств и методов[3].

С практической стороны применения информационных систем можно отметить, что сама информационная система является лишь инструментом,

---

[1] Павлюков В.В. Организационно-правовые основы противодействия кибератакам на инфраструктуру государства // Вестник Московского университета. Серия 11: Право. - 2019. - № 4. – С. 126.

[2] Вязовец Р.Н. Использование информационных технологий в оперативно-розыскной деятельности органов внутренних дел: автореф. дис. … канд. юрид. наук: 12.00.09 / Вязовец Роман Николаевич. – М., 2010. – С. 3.

[3] Демина Р.Е. Информационное обеспечение раскрытия преступлений: пути оптимизации // Вестник Поволжской академии государственной службы. – 2008. – № 3. – С. 83.

который призван помочь сотруднику ОВД при расследовании, раскрытии, а иногда и при предотвращении преступлений.

Задачи по формированию и ведению централизованных учетов, баз данных оперативно-справочной, розыскной, криминалистической, статистической и иной информации, а также обеспечение межведомственного и межгосударственного информационного взаимодействия возлагаются на информационно-аналитические подразделения органов внутренних дел. В структуре МВД России для этих целей создано и функционирует Федеральное казенное учреждение «Главный информационно-аналитический центр МВД России»[1].

В марте 2012 года МВД утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России. Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства.

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы ОВД, который велся с 2005 года. Основной составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и госорганами различных уровней[2].

«Важнейшим шагом по развитию современных технологий, стало создание Единой информационно-телекоммуникационной системы органов внутренних дел. Ее практическое внедрение обеспечивает широчайшие информационные возможности: от быстрого получения информации из специализированных баз данных федерального и регионального уровней до проведения видеоконференций и дистанционного обучения для сотрудников органов внутренних дел. По данным

[1] Об утверждении устава федерального казенного учреждения «Главный информационно-аналитический центр министерства внутренних дел Российской Федерации: Приказ МВД России от 31 декабря 2010 № 910 [Электронный ресурс] // Официальный сайт МВД РФ. – URL: https://mvd.ru/upload/site1/folder_page/006/825/743/Prikaz_910-GIATs.doc (дата обращения: 26.02.2025).

[2] Единая система информационно-аналитического обеспечения деятельности МВД РФ Ход проекта [Электронный ресурс]. – URL: http://www.tadviser.ru/index.php/Проект:Единая_система_информационно-аналитического_обеспечения_деятельности__МВД_РФ_(ИСОД_МВД) (дата обращения: 04.02.2025).

Пресс-центра МВД России, активное ее внедрение способствовало раскрытию более третьей части от общего числа расследованных преступлений»[1].

Постепенно обеспечение повышения эффективности функционирования инфокоммуникационных систем в оперативно-служебной деятельности органов внутренних дел стало возможным, в первую очередь, благодаря созданию и ведению компьютерных Банков данных в каждом подразделении ОВД.

Банк данных – это автоматизированная информационная система, включающая в свой состав комплекс специальных методов и средств (математических, информационных, программных, языковых, организационных и технических) для поддержания динамической информационной модели предметной области с целью обеспечения информационных запросов пользователей[2]. Уже сейчас в органах внутренних дел России созданы и функционируют региональные, межрегиональные и федеральные автоматизированные Банки данных информации.

Первоначальным этапом использования Банков данных является этап сбора и накопления информации, законодательно регламентированный ст. 17 ФЗ «О полиции». Перечень лиц, о которых разрешено собирать сведения в Банки данных МВД, закреплен этой же статьей. В п. 1 ст. 17 также указано, что полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в Банки данных[3].

Зачастую процесс накопления информации в информационных системах ОВД начинается после или в момент заявления о совершении преступления.

Анализируя ст. 17 ФЗ РФ «О полиции», можно сделать вывод, что целью таких Банков в МВД РФ является накопление информации о лицах и о деяниях, которые они совершили ранее. В свою очередь, органы, осуществляющие

---

[1] Посков Я.А. Роль единой информационно-телекоммуникационной системы органов внутренних дел в информационном обеспечении производства следственных действий // Известия Тульского государственного университета. Экономические и юридические науки. 2009. №. 1. С. 338-342. С.339.

[2] Карпова И.П. Базы данных: учебное пособие. – СПБ.: – Питер, 2013. – С. 17.

[3] О полиции: Федеральный закон от 07 февраля 2011 № 3-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

оперативно-розыскную деятельность, для решения возложенных на них задач могут создавать и использовать информационные системы на основании ст. 10 ФЗ «Об оперативно-розыскной деятельности»[1].

На практике вся информация о лице заносится в Банки данных в ручном режиме и только после того, как лицо совершило некое деяние. Зачастую источником информации является лишь заведенная на лицо карточка. Впоследствии информация, занесенная в Банк данных сотрудником органа внутренних дел, может не пополняться годами из-за отсутствия источника получения информации. В связи с устаревшими данными в Банках данных МВД при раскрытии и расследовании преступлений оперативный сотрудник ОВД вынужден прибегать к поиску альтернативных источников для получения актуальной оперативно-значимой информации.

Наверное, именно поэтому А.Д. Ульянов отмечает, что не всегда обеспечивается современный сбор и анализ информации о процессах и явлениях, влияющих на состояние, уровень и динамику преступности, выработка на этой основе управленческих решений. Органы внутренних дел существенно проигрывают в оперативности, злободневности анализа[2].

С помощью учетов информационных центров УВД, ГУВД, МВД информационные потребности оперативно-розыскной деятельности ОВД удовлетворяются лишь частично, отмечает Р.Х. Якупов. В указанных учетах содержатся данные только о лицах и фактах, имеющих отношение к уже выявленным и зарегистрированным преступлениям и лицах, их совершившим. Вместе с тем, лица, ранее судимые, составляют около трети общего объема ежегодно регистрируемых преступников. Возможность получения легких денег (закладчики наркотических средств, дропы), привели к тому, что на путь совершения преступлений встала большая часть ранее законопослушных граждан. Поэтому для выявления новых преступлений и лиц, их совершивших, необходима

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (с изм. и доп.) [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[2] Ульянов А.Д. Информационно-аналитическое обеспечение управленческой деятельности в органах внутренних дел // Вестник ВИ МВД России. – 2007. – № 1. – С. 37.

более обширная информация, а не только данные о лицах, взятых на централизованный учет[1].

Ситуация, которая складывается в деятельности ОВД, требует усовершенствования подходов к использованию результатов ОРД с целью организации борьбы с преступностью. Они должны базироваться на глубоком системном анализе разноплановой оперативно-значимой информации, которая обеспечивала бы эффективное противодействие преступлениям. Важная роль в этом процессе принадлежит алгоритмичному применению сведений информационных систем и обоснованию соответствующих рекомендаций по совершенствованию информационно-аналитического аспекта противодействия преступности.

Эффективная борьба ОВД с преступностью возможна лишь при условии дальнейшего развития специальных научных знаний, разработки действенных методов и современных научно-технических средств получения, обработки и фиксации доказательной информации. Поэтому закономерно возникает вопрос о необходимости фиксировать в Банках данных результаты ОРМ.

На практике сотрудник органов внутренних дел при выполнении своих служебных обязанностей, имея компьютер и доступ к ведомственной компьютерной сети, непременно обращается к учетам, которые накоплены при помощи информационных систем (ИСОД), функционирующих в МВД РФ. После авторизации в Банке банных МВД сотрудник полиции при наличии анкетных данных об интересующем лице, а именно фамилии, имени, отчестве, дате, месяце и годе рождения, может сделать запрос и зачастую получить исчерпывающий перечень информации об анкетных данных, месте проживания, и деяниях, которые запрашиваемый совершил ранее. Благодаря возможностям информационных систем, сотрудник ОВД, не имея полных анкетных данных, может запросить информацию с теми данными, которыми он располагает, например, фамилией и адресом проживания. Некоторые Банки данных позволяют искать лицо по кличке или возможно сделать выборку лиц, проживающих на определенном адресе.

[1] Якупов Р.Х. Некоторые особенности понятия информационного обеспечения деятельности оперативных подразделений органов внутренних дел по раскрытию краж из квартир // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2010. – № 1(12). – С. 203.

Бесспорно, безграничные возможности обработки информации может дать грамотно сконфигурированная модель управления информационными процессами в появляющихся современных технологиях. Однако, до сих пор исключением является невостребованность информационно-аналитического механизма обработки данных в повседневной деятельности сотрудника полиции в борьбе с преступностью, совершаемой при помощи информационных технологий. Это связано с тем, что действия в Глобальной компьютерной сети не фиксируются в Банках данных ОВД.

Становится актуальным вопрос об оптимизации информационно-справочного обеспечения раскрытия и расследования преступлений с использованием комплекса информационных систем, поиска научных продуктов, позволяющих быстро получать, обрабатывать и фиксировать значительные объемы гласных результатов ОРД; эффективно разыскивать, выделять и анализировать признаки искомых объектов; моделировать динамические процессы, вероятные ситуации; интегрировать распределенные информационные системы органов внутренних дел и других учреждений и организаций, а также стадии экспертного исследования; повышать научную обоснованность и объективность информационного поиска.

Однако при разработке и внедрении таких систем приходится сталкиваться с проблемами законодательного характера, которые на практике не так уж и просто разрешить. Прежде всего, это объясняется тем, что сотруднику ОВД, чтобы выявить и зафиксировать факт преступления, совершаемого при помощи информационных технологий, приходится работать с огромными потоками социально-правовой информации, справиться с которыми без помощи современных технических и программных средств практически невозможно[1].

В целях разрешения этой проблемы стоит проанализировать законодательство и научные разработки, связанные с поступлением фото- и видеоизображений, а также всевозможной другой компьютерной информации в

[1] Бурцева Е.В., Рак И.П., Селезнев А.В., Терехов А.В. Роль информационных технологий в профилактике и раскрытии преступлений // Вестник ТГУ. – 2008. – № 2. – С. 479.

подразделения органов внутренних дел и обозначить возможные направления ее решения.

Анализируя научные исследования, мы можем заключить, что отдельные ученые также обеспокоены существованием данной проблемы. Так, А.Ю. Архипов, рассматривая деятельность ОВД при сборе видеоматериалов территориальными ОВД, указывает на то, что практически не проводятся специальные видеозаписи задержанных лиц. По мнению исследователя, сбор видеотеки позволил бы комплексно использовать видеоматериалы при отождествлении личности, охватив все ее идентификационные признаки и свойства[1].

В этом направлении закон также не выступает на стороне правоохранительных органов. Вот, к примеру, что говорится в ст. 24 Конституции Российской Федерации – «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»[2].

Аналогично в ст. 152.1 Гражданского кодекса РФ «Охрана изображения гражданина» указано, что «Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина»[3].

Однако фото- и видеоматериалы могут накапливаться и храниться в банках данных ОВД на основании ФЗ «О полиции» и ФЗ «О государственной дактилоскопической регистрации в Российской Федерации», где установлен исчерпывающий перечень оснований, при наличии которых в отношении граждан возможно проведение дактилоскопирования и фотографирования.

Так, в соответствии с п. 19 ст. 13 ФЗ «О полиции» сотрудникам полиции

---

[1] Архипов А.Ю. Основные направления и проблемные вопросы использования банков данных видеоинформации в деятельности оперативных подразделений при раскрытии преступлений // Вестник Нижегородской академии МВД России. – 2015. – № 1(29). – С. 214.

[2] Конституция Российской Федерации от 12 декабря 1993 года [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[3] Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.02.2025).

предоставлено право производить регистрацию, фотографирование, аудио-, кино- и видеосъемку, дактилоскопирование лиц, задержанных по подозрению в совершении преступления, заключенных под стражу, обвиняемых в совершении преступления, подвергнутых административному наказанию в виде административного ареста, иных задержанных лиц, если в течение установленного срока задержания достоверно установить их личность не представилось возможным[1].

В ст. 6 ФЗ «Об оперативно-розыскной деятельности» обозначено, что в ходе проведения оперативно-розыскных мероприятий могут использоваться 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[2].

Исходя из вышеуказанного, можно сделать вывод, что процесс наполнения Банков данных ОВД различной информацией, в том числе фото- и видеоматериалами сильно ограничивается тем, что основания для фотографирования лица или фиксация его при помощи различных технических средств производится только в ограниченном законом порядке.

Расширение области получения компьютерной информации видится необходимым и оправданным действием. В настоящее время в органах внутренних дел России созданы условия для накопления фотоизображений с целью дальнейшего их сопоставления в процессе опознания лица, где используется несколько габитоскопических регистрационно-поисковых систем. Н.Л. Щеголева и А.К. Туяка в своей научной статье отметили две наиболее совершенные в техническом плане системы – «Портрет-Поиск» и «Сова»[3].

Автоматизированная информационно-поисковая система (далее – АИПС)

---

[1] О полиции: Федеральный закон от 07 февраля 2011 № 3-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

[3] Щеголева Н.Л., Туяка А.К. К вопросу совершенствования современных габитоскопических регистрационно-поисковых систем / Вестник Санкт-Петербургского университета МВД России. – 2013. – № 3(59). – С. 225.

«Портрет-Поиск» позволяет в считанные минуты проводить поиск по четырем направлениям: «лицо-лицо», «лицо-портрет», «портрет-портрет» и «портрет-лицо», для чего используются формализованные (словесные – возраст, рост, телосложение и прочие) и графические параметры лица (по 18-ти точкам)[1].

Уже сейчас мы можем наблюдать как АИПС «Портрет-Поиск» дает положительные результаты в борьбе с преступностью.

Так, около дома по ул. Черняховского г. Хабаровска неизвестный напал на женщину и, вырвав сумку, скрылся с места происшествия. В тот же день потерпевшая была направлена в ЭКЦ УМВД России по Хабаровскому краю для составления субъективного портрета. При дальнейшей проверке портрета по базе лиц АИПС «Портрет-Поиск» сотрудниками полиции было установлено лицо, предположительно причастное к совершению данного преступления. В ходе проверки 44-летний гражданин был задержан, установлена его причастность к совершению грабежа[2].

Аналогичная система также существовала и в подразделениях других государств, например, в Управлении Информационно-аналитического обеспечения (далее – УИАО) ГУМВД Украины в Луганской области, которое долгое время являлась передовиком по созданию информационных систем на Украине[3].

Так, в упомянутом УИАО была внедрена Биометрическая система идентификации граждан по изображению лица «АРГУС». Система «АРГУС» позволяла установить тождественность неизвестного объекта известному на основании совпадения признаков в любом фотоизображении, которое будет участвовать в процессе биометрического опознания[4].

Основным источником биометрических шаблонов базы данных системы

---

[1] МВД РФ создает поисковую систему, которая позволит по фотороботу быстро найти человека [Электронный ресурс]. URL: http://www.newsru.com/russia/24sep2008/proekt.html (дата обращения: 15.01.2025).

[2] Полицейские Хабаровского края рассказали о работе автоматизированной информационно-поисковой системы «Портрет-Поиск» от 13.08.2015 [Электронный ресурс]. – URL: https://27.mvd.ru/news/item/6328745/ (дата обращения: 29.01.2025).

[3] Павлюков В.В. Правовые и организационные основы использования единой информационно-аналитической системы в ОВД // Вестник Костромского государственного университета имени Н.А. Некрасова. – 2017. – № 3. – С. 274.

[4] Павлюков В.В. Перспективы использования полицией ЛНР современных информационных технологий в противодействии преступности // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2016. – № 1 (1). – С. 266.

«АРГУС» являются:

- фотопортрет лица, представленный в цифровом виде (графический файл);

- фотография портретного типа (для дальнейшего сканирования);

- цифровой «видеопоток» (отдельный фрагмент в виде медиафайла, или видеосигнала, который поступает в реальном времени)[1].

Однако процесс распознавания в системе начинается после того, как фото- или видеоданные в цифровом виде поступят в банк данных УИАО. Специально обученный сотрудник отмечает определенные биометрические данные на фотоизображении и только после этих действий программа начнет поиск в базе данных УИАО. Хотя этот процесс занимает длительный промежуток времени, однако тоже дает положительный результат.

Например, в г. Луганске при помощи видеокамеры, установленной в банкомате, был зафиксирован видеофакт использования «белого пластика» (поддельных пластиковых карт), при помощи которого преступник в банкомате снимал деньги. Данное видео было направленно в УИАО ГУМВД Украины в Луганской области, где при помощи «АРГУС» путем сопоставления цифровых данных, полученных из банкомата, с учетами, которые велись в УИАО, была установлена личность гражданина, совершившего данное преступление[2]. Забегая вперед, необходимо указать, что программное обеспечение в банкомате фиксирует использование «белого пластика», и, если регулярно предоставлять в ОВД эти данные, например, раз в сутки, то количество раскрытых преступлений, совершаемых таким способом, может значительно повыситься.

Как указывалось, ранее, основной проблемой Банков данных МВД является правовое ограничение использования фото- и видеоматериалов, а также ограничены источники получения цифровой информации, которые могут участвовать в обработке данных и быть предоставлены для установления лица и

---

[1] Современное оружие сотрудников органов внутренних дел: информационные технологии как ответ на вызов времени: практ. пос. / Ю.А. Задорожний, А.Е. Трубкович, О.В. Колтырин, и др. / МВД Украины, Луганский государственный университет внутренних дел им. Э.А. Дидоренко. – Луганск: РИО ЛГУВД им. Э.А. Дидоренко, 2012. – С. 64.

[2] Павлюков В.В. Оперативное распознавание лица по фото-, видео- и аудиоданным: перспективы внедрения современных технологий в деятельности органов внутренних дел // Вестник Костромской государственный университет имени Н.А. Некрасова. – 2016. – № 6. – С. 207.

фиксации его преступной деятельности. Для того, чтобы выйти из данной ситуации, необходимо использовать возможности получения компьютерной информации из альтернативных источников. Наиболее подходящим источником таких данных может послужить Глобальная сеть Интернет с задействованием искусственного интеллекта.

Уже сегодня, по алгоритмам ранее совершенных преступлений искусственный интеллект может создать модель поведения преступника, на всех этапах проведения расследования организовать сбор как основной, так и дополнительной доказательственной базы на основе уже имеющейся, составить планы проведения расследования на первоначальном и последующем этапе, осуществляя анализ, технический и логический контроль составления.

Что касается адаптации искусственного интеллекта для решения специфических криминалистических задач, то такими задачами могут быть:

1) разработка и планирование порядка проведения как одного, так и ряда следственных действий с использованием методической базы по проведению расследования как в целом, так и в частности;

2) проведение анализа материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера и разработки путей устранения уже имеющихся ошибок и недопущения их в будущем (машинное обучение). Дальнейшая разработка возможностей многоуровневой архитектуры искусственного интеллекта позволит провести интеграцию компьютерной технологии в криминалистическую практику. На отдельных этапах цифровизации расследования преступлений автоматизированные информационно-поисковые системы с использованием технологий искусственного интеллекта и нейросетей способствуют существенному повышению эффективности расследования путем автоматизации деятельности правоохранительных органов, организации расследования преступлений, анализа информации, принимают на себя часть когнитивной деятельности следователя и позволяют значительно снизить сроки на принятие решений в определенных ситуациях без потери

качества[1].

Положительный эффект от использования искусственного интеллекта, можно наблюдать в Главном следственном управлении по Свердловской области, где искусственному интеллекту (GPT) были предоставлены материалы уголовного дела, на основе которых ему предложено выдвинуть версии и разработать программу расследования преступления на начальном этапе. Искусственный интеллект достаточно детально и объективно проанализировал, а также спланировал мероприятия, необходимые для раскрытия и расследования преступлений. Он также может помочь в формировании вопросов для экспертизы и определении различных видов экспертиз, пишет Р.С. Хамидуллин[2].

К сожалению, пока законодатель четко не обозначил процесс обработки и фиксации информации, которая находится в открытом доступе в сети Интернет сотрудниками ОВД. Проведенный нами ранее анализ научных трудов по этому вопросу позволяет предположить, что, если пользователь Интернета на ресурсах сети (блогах, форумах, социальных сетях, видеохостингах и т. д.) добровольно оставил данные о себе, то он должен осознавать тот факт, что информация может просматриваться всеми, кто имеет доступ к ресурсу, где размещены данные о нем, и поэтому не подлежит судебной защите. Можно также сослаться и на п.35 ст. 13 ФЗ «О полиции», исходя из которого сотрудник полиции может использовать на безвозмездной основе возможности средств массовой информации и информационно-телекоммуникационной сети Интернет для размещения информации в целях установления обстоятельств совершения преступлений, лиц, их совершивших, а также для розыска лиц, скрывшихся от органов дознания, предварительного следствия или суда, и лиц, пропавших без вести. Сотруднику ОВД необходимо взять на вооружение данные, размещенные в сети Интернет, выработать механизм использования информации при поиске и фиксации лиц с целью раскрытия и расследования преступлений. И поэтому не лишним будет

[1] Смушкин А.Б. Отдельные аспекты использования искусственного интеллекта в криминалистической деятельности // В сборнике: Следственная деятельность. сборник научных трудов. – Минск, 2023. – С. 309-310.

[2] Хамидуллин Р.С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Электронное приложение к Российскому юридическому журналу. – 2024. – № 2. – С.23.

добавить в п.35 ст. 13 ФЗ «О полиции» после слова «размещения» – «и получения».

К счастью, такой механизм получения компьютерной информации частично реализован частными компаниями. Уже сейчас в Интернете существуют и активно используются множество сервисов, которые позволяют осуществлять поиск компьютерной информации одновременно в различных ресурсах сети Интернет. Одним из таких является – social-searcher.com, призванный сократить время анализа различных соцсетей (Twitter, Instagram, YouTube, Flickr, Facebook). При помощи social-searcher можно указать поисковые запросы, исключить какие-то слова, выбрать тип контента, который вам нужен, – фото, видео, ссылки и так далее, а также получать письма-оповещения о новых результатах[1].

Для распознавания по фото подойдет такой сервис Google, как «картинки-Google», позволяющий осуществлять в режиме реального времени поиск цифровых фотографий и картинок по всем сайтам сети Интернет. Для того, чтобы воспользоваться этим сервисом, нет необходимости использовать специальные навыки и умения. Пользователю необходимо перейти на страницу сервиса и загрузить картинку. Сервис предоставит вам список сайтов, где не только встречается идентифицируемая картинка, но также предоставит схожие изображения.

Для более эффективного раскрытия преступлений, совершенных в сфере компьютерной информации, необходимо обратиться к широкому кругу возможностей различного программного обеспечения[2]. Относительно недавно российскими программистами был создан программный продукт «FindFace», который был представлен как сервис знакомств по фотографии. За считанные мгновения технология сравнивает фотографию человека с миллионами снимков, которые хранятся в открытом доступе в Интернете и максимально точно находит схожие изображения, причём, вне зависимости от угла съёмки, света, и положения

[1] Social Searcher Free Social Media Search Engine [Электронный ресурс]. – URL: https://www.social-searcher.com/ (дата обращения: 19.01.2025).

[2] Соколов А.Б., Щербина Р.П., Шаевич А.А. Криминалистически значимая информация, хранящаяся в альтернативных потоках данных файловой системы NTFS // Криминалистика: вчера, сегодня, завтра. – 2022. – № 2 (22). – С.161.

головы. «В 300 миллионной базе фотографий точность 70 процентов», – сообщает Артем Кухаренко, основатель компании N-Tech.Lab[1]. Для того, чтобы использовать программу «FindFace», ее достаточно установить в смартфон, запустить и сфотографировать лицо человека.

Не стоит упускать из вида программы для распознавания речи, которых также огромное количество и которые практически не нашли применения в деятельности ОВД. Например, в Яндексе используется приложение «Яндекс-Диктовка» для перевода устной речи в текст. Возможности данной программы позволяют распознавать и синтезировать русскую речь, выделяя семантические объекты в тексте[2].

Отдельно стоит остановиться на использовании мессенджера «Telegram», который активно используют в своей деятельности злоумышленники. Для получения компьютерной информации о жертве преступники используют Telegram-бот «Глаз Бога». Зная номер телефона, злоумышленник может получить компьютерную информацию о жертве в социальных сетях и коммерческих сервисах «Вконтакте», «Skype», «Одноклассники», «WhatsApp», «Telegram», «GetContac»t, «NumBuster», «TrueCaller», в объявлениях на Avito, Youla, Auto, Cian и пр. Кроме того, сервис позволяет отправить анонимное SMS-сообщение, а за 15 рублей получить образец голоса абонента. При выборе подобной услуги абоненту поступает звонок, определяющий доступность телефона, и в случае, если абонент принял вызов, включается диалог с голосовым роботом. Файл с записью голоса поступает инициатору запроса сразу после завершения диалога, длительность составляет 10 секунд, при этом можно выбрать сценарий звонка — «мужчина», «девушка», «грубый», «наглый», «школьник», «курьер»[3]. Данный сервис также стоит взять на вооружение и сотрудникам правоохранительных органов, с целью получения информации о злоумышленнике.

---

[1] FindFace: российская программа распознавания лиц завоевывает мир [Электронный ресурс]. – URL: http://www.vesti.ru/doc.html?id=2723304 (дата обращения: 09.01.2025).

[2] Яндекс-Диктовка [Электронный ресурс]. – URL: http://speech-soft.ru/prog/yandeksdiktovka (дата обращения: 29.01.2025).

[3] За кулисами мошенничества [Электронный ресурс]. Сайт sberbank.ru URL: https://www.sberbank.ru/ru/person/kibrary/investigations/berdyansk-glava-5 (дата обращения: 07.03.2025).

Сейчас мы можем видеть, какие возможности нам дают компьютерные технологии. На законодательном уровне важно закрепить и задействовать всевозможные источники получения компьютерной информации. На практике стоит автоматизировать, насколько это возможно, не только обработку, но и поступление значимой для расследования информации в ОВД при помощи современных компьютерных технологий, а также обязательно проработать механизм фиксации полученных результатов и правильного их процессуального оформления. Даже при разработке системы искусственного интеллекта на базе искусственной нейронной сети первоначально происходит формирование базы данных, которая будет использована для дальнейшего обучения[1].

Практика использования совмещения компьютерной информации оперативно-розыскного значения с информацией из ресурсов сети Интернет была удачно внедрена и использована сотрудниками Управления информационных технологии (далее – УИТ) г. Луганска. Приведем пример, где были проанализированы интернет-сайты и форумы, имеющие отношение к Луганской области, тематикой которых являлись вопросы, связанные с оружием, боеприпасами и т. д.

При анализе информации был установлен сайт «www.Reibert.info», на котором заинтересованные лица имеют возможность обмениваться информацией на военную тематику. В разделе «Форум-военная археология-находки» было выявлено лицо, зарегистрированное на сайте под логином гр. «И», с информацией относительно проведенных ею раскопок в Донецкой области на предмет нахождения оружия и боевых припасов времен Великой Отечественной войны. Подтверждая информацию о найденных вещах, это лицо опубликовало фотоизображение боевых припасов времен Великой Отечественной войны – гранат, минометных мин, автоматов, пистолетов, боеприпасов к автоматам и пулеметам.

С целью установления анкетных данных лица, зарегистрированного на

[1] Степаненко Д. А., Бахтеев Д. В., Евстратова Ю. А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. – 2020. – №. 2(14). – С. 206-214. – С. 211.

данном сайте, была проанализирована информация на странице последнего. При анализе информации на личной странице гр. «И» установлено, что он родился 05.05.1975 года, живет в г. Северодонецке Луганской области, занимается поиском мест боевых действий, по профессии слесарь, зарегистрировался на сайте «www.Reibert.info» 12.12.2008 года и ежедневно проявлял активность на данном сайте.

Для получения дополнительной характеризующей информации об этом лице проанализирована информация, содержащаяся в переписке на форуме. Анализ переписки позволил установить, что данное лицо использует возможности сайта для покупки-продажи найденных боеприпасов и оружия.

Для идентификации лица проведена выборка лиц по учетам УИТ УМВД с использованием полученной информации: дата рождения, место проживания, род занятий – слесарь. В ходе проведенной выборки лиц был установлен гр. «А» с заданными параметрами года рождения и места жительства, по профессии слесарь, ранее пять раз судимый за мошенничество, незаконный оборот оружия и подделку документов (ранее гр. «А» был задержан сотрудниками ОВД, в ходе досмотра у него было обнаружено самодельное огнестрельное оружие).

На основании вышеизложенного, учитывая имеющиеся каналы поступления оружия и боевых припасов (археологические раскопки), возможности ремонта найденного оружия и боеприпасов (используя профессиональные навыки слесаря), сотрудниками УИТ выдвигается аргументированное предположение о причастности гр. «А» к незаконному обороту оружия, боеприпасов и взрывчатых веществ с использованием возможностей сети Интернет, а именно, сайта «www.Reibert.info».

Полученная информация была сформирована в справку по принципу «досье» и направлена в оперативное подразделение УМВД.

В ходе проверки данной информации оперативными сотрудниками УМВД в Луганской области был проведен комплекс оперативно-розыскных мероприятий, нацеленных на проверку гр. «А» и его возможных связей на причастность к незаконному обращению оружия, боеприпасов и взрывчатых веществ с

использованием возможностей сети Интернет, а именно, сайта «www.Reibert.info». Впоследствии были проведены санкционированные обыски по месту жительства гр. «А» и его связей, в ходе которых были обнаружены и изъяты в больших количествах огнестрельное оружие, боеприпасы, взрывчатые вещества времен ВОВ, которые гр. «А» и его связи хранили с целью последующего сбыта. По данному факту возбуждено уголовное дело[1].

Задействование Банков данных ОВД в связке с вневедомственными информационными системами, как мы можем видеть из приведенных примеров, уже сейчас способствует оперативному расследованию и раскрытию преступлений. Однако мы считаем, что данный процесс можно и нужно автоматизировать.

Используя алгоритмы работы вышеуказанных сервисов, мы можем моделировать ситуацию, когда в поле зрения сотрудников ОВД попадают, например, экстремистские материалы, передаваемые в сети в форме музыкальной композиции или запечатленные на видео, которые возможно зафиксировать при помощи ОРМ «Получение компьютерной информации». Задействуя технологии, которые используются в программе распознания речи «Яндекс-Диктовка», аудиокомпозицию можно преобразовать в текстовый файл и сверить с федеральным списком экстремистских материалов без участия лингвиста. При наличии имеющейся фотографии лица, разместившего аудиозапись или видеофайл, используя АИПС «Портрет-Поиск», «АРГУС» и программу «FindFace», возможно оперативно провести поиск лица по всем имеющимся учетам ОВД и в сети Интернет соответственно. Установить дополнительные данные о лице возможно при помощи программы Social-searcher и схожих с нею сервисов, при этом проверить пользователя на наличие размещенной им противоправной информации на других ресурсах Интернета. По результатам будет предоставлен портрет преступника. Сотруднику ОВД останется только сформировать и распечатать протокол получения компьютерной информации. В свою очередь,

[1] Павлюков В.В. Некоторые методики раскрытия и расследования преступлений с использованием информационно-поисковых систем ОВД и компьютерной информации из сети Интернет // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2017. – № 2. – С. 164.

компьютерные технологии позволяют сделать так, чтобы в протоколе были зафиксированы и отображены все необходимые процессуальные реквизиты, которые требует ст.166 УПК РФ. Ведь, как справедливо отмечают В.Д. Зеленский и Г.М. Меретуков, использование современных Банков данных эффективно при решении самых различных аналитических задач, в частности, связанных с составлением наиболее сложных процессуальных документов. Решение этой задачи предполагает использование не только текстовых редакторов, но и автоматизированных информационно-поисковых систем, позволяющих формировать текст, группируя собранные доказательства[1].

Можно отметить такой обязательный факт, что Банк данных является многопользовательской информационно-поисковой системой, не только состоящей из одной или нескольких баз, но также умеющей получать информацию из различных баз данных, обладать возможностью динамического и постоянного поиска и постоянного мониторинга информационных источников, иметь привилегированную систему хранения, обработки, управления и поиска информации в ней.

Накопление и использование учётных данных о внешнем облике преступника не является самоцелью, а лежит в плоскости достижения той цели, ради которой и существуют Банки данных – информационного обеспечения по установлению личности преступника и фиксации результатов его противоправной деятельности.

Эффективность такой деятельности зависит не только от полноты сосредотачиваемой в учётах ОВД информации, но и от чёткой систематизации учётных данных, их автоматизации и интеграции, от продуктивного взаимодействия различных служб в этом вопросе. Немаловажным является и оперативное предоставление запрашиваемой информации на фигурирующих в деле лиц в режиме реального времени из вневедомственных источников[2].

---

[1] Криминалистика: учебник / под ред. д.ю.н., профессора В.Д. Зеленского и д.ю.н., профессора Г.М. Меретукова – СПб, Издательство «Юридический центр», 2015. – С. 240.

[2] Бусов А.В. Использование габитоскопических учётов в раскрытии, расследовании и предупреждении преступлений // Вестник Санкт-Петербургского университета МВД России. – 2011. – № 4. – С. 79.

При раскрытии и расследовании преступлений сотрудниками ОВД РФ альтернативными источниками получения оперативно-значимой компьютерной информации выступают не только Банки данных в системе МВД, но и ресурсы сети Интернет. Приведенные практические примеры свидетельствуют о том, что данные, полученные из сети Интернет, сотрудникам ОВД приходится в ручном режиме сопоставлять и анализировать с данными, которые накоплены в Банках данных МВД РФ и направлять запросы владельцам интернет-ресурсов, операторам связи и провайдерам. Этот процесс усложняется и тем, что сотрудникам полиции не хватает времени и навыков на анализ и обработку информации, которую предоставляет Интернет.

Из вышеуказанного следует, что проблема автоматического наполнения оперативными данными о гражданах в Банках данных ОВД и сравнительный анализ полученной информации из различных интернет-источников является актуальной в связи с развитием социальной популярности данной отрасли. Поэтому актуальность поиска новых информационных источников, создание механизмов получения данных и автоматический анализ информации является основанием не только для того, чтобы наполнить Банки данных ОВД информацией о лице, но и для предотвращения преступлений.

По мнению 98 % опрошенных сотрудников ОВД процесс получения информации при объединении компьютерной информации из сети Интернет с банками данных ОВД придаст оперативности в противодействии преступности[1].

83% опрошенных нами сотрудников ОВД считают, что обмен информацией между сотрудниками ОВД при условии предоставления и передачи информации с использованием компьютерных сетей ускорит оперативность работы ОВД в целом, 13% процентов ответили негативно и 4% воздержались[2].

Автоматизации при наполнении Банков данных ОВД РФ оперативно-значимой информацией из сети Интернет возможно достичь путем решения следующих задач:

---

[1] См.: Приложение № 1. Опросный лист.
[2] См.: Приложение № 1. Опросный лист.

- анализа существующих современных технологий при автоматизации обмена информацией;

- анализа действующего законодательства на предмет получения и использования данных из альтернативных источников для занесения в Банки данных ОВД РФ;

- возможности правового и практического применения данных при объединении Банков данных ОВД, интернет-сайтов и операторов связи.

Примером механизма поиска и фиксации информации в сети Интернет могут послужить поисковые системы с мировым именем, такие как Google, Яндекс, Mail.ru и т. д., которыми, чтобы проиндексировать и в дальнейшем выдать интересующий контент по запросу, применяется механизм парсинга.

Парсинг сайтов – последовательный синтаксический анализ информации, размещённой на интернет-ресурсах, позволяющий выделить нужный контент.

Полученный в ходе парсинга результат может предоставляться, например, в виде базы данных или электронной таблицы[1].

Как видим, возможности современных технологий позволяют получать и анализировать общедоступные данные о пользователях в автоматическом режиме, но остается не решенным вопрос законности сбора такой информации правоохранительными органами и не раскрыты возможные механизмы получения этих данных из Интернета.

Мы считаем, что данные, которые пользователь после регистрации самостоятельно оставил на том или ином интернет-ресурсе, являются общедоступными персональными данными. В свою очередь в соответствии со ст. 3 ФЗ от 27.07.2006 г. № 152-ФЗ «О персональных данных» общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с ФЗ не распространяется требование соблюдения конфиденциальности[2].

---

[1] Парсинг: Что? Зачем? Как? [Электронный ресурс]. URL: http://parsing.valemak.com/ (дата обращения: 22.01.2025).

[2] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ [Электронный ресурс] //

С целью автоматизированного пополнения Банка данных МВД и фиксации противоправной деятельности автор предлагает получать и обрабатывать информацию из сети Интернет путем рассмотренного выше механизма-парсинга. То есть, программа-парсер будет выступать от имени зарегистрированного пользователя и в автоматическом режиме сопоставлять информацию, которая находится в Банках данных МВД РФ с информацией, которая хранится в сети Интернет, и, в случае сходства данных, будет объединять их.

Мы предполагаем, что это может стать возможным благодаря продуманной системе организации работы ОВД, создания законных оснований и усовершенствования механизма функционирования Банков данных МВД РФ.

В целях законного использования информации, полученной из интернет-ресурсов, целесообразно дополнить ст. 17 ФЗ «О полиции» пунктом следующего содержания: «Полиция имеет право вносить в Банки данных и использовать в своей деятельности информацию о лицах, полученную из сети Интернет». Такой законодательный шаг создаст возможность автоматизировать объединение данных, которые уже имеются в Банках данных МВД РФ с информацией, находящейся на сайтах сети Интернет. При этом увеличится объем дополнительной, и, что немаловажно, динамически обновляемой компьютерной информации оперативно-розыскного значения о лице.

Объединение данных даст возможность не только автоматизировать процесс наполнения информацией Банков данных МВД РФ, но и постоянно отслеживать деятельность лиц, подозреваемых в совершении преступлений, расширит представление об их преступных связях, и, что очень важно, позволит предотвратить готовящееся преступление[1].

Для урегулирования этой проблемы предлагается внедрить систему мониторинга интернет-«трафика», с помощью которой можно получать, фиксировать, хранить и проводить анализ информации о посещении

Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 23.01.2025).

[1] Павлюков В.В. Правовая и практическая возможность объединения данных в информационно-поисковых системах МВД РФ с информацией из сети Интернет // Вестник Костромского ГУ им. Н.А. Некрасова МВД России. – 2016. – № 3. – С. 227-229.

пользователями пространства Глобальной сети в реальном времени, в первую очередь сайтов с запрещенным материалом.

78 % опрошенных нами оперативных сотрудников считают, что оперативный интерес будут иметь граждане, которые обращались к Интернет-ресурсам с запрещенным материалом, 12 % так не считают и 10 % воздержались[1].

Рассматривая Интернет как источник получения информации, нужно отметить и помощь провайдера в получении доступа к компьютерной информации. Так, данные могут даже не храниться на сервере провайдера, а сразу передаваться на специально выделенный удаленный сервер хранения LOG-файлов.

Полученная информация может быть состыкована с базами данных, которые используют в своей деятельности правоохранительные органы, что в реальном времени позволит:

1. Установить пользователей, посещавших ресурс, на котором может совершаться противоправная деятельность, а также IP-адрес и время его посещения.

2. Отследить сетевую активность и интересы пользователя.

3. Установить местонахождение компьютерного устройства.

4. Выявлять причастных к совершению преступных действий пользователей.

В свою очередь, лиц, предоставляющих услуги хостинга, и владельцев ресурсов Российского сегмента сети также необходимо обязать вести логирование посещений ресурсов. Если есть подозрение, что с помощью ресурса сети происходят противоправные действия, то, по первому требованию уполномоченных правоохранительных органов, владелец хостинга должен предоставить информацию правоохранительным органам[2], а в случае отсутствия возможности предоставить такие данные, должен предоставить полный доступ к ресурсу, передав все логины и пароли правоохранительным органам. С этим согласны 94 % процентов опрошенных нами оперативных сотрудников ОВД[3]. В

[1] См.: Приложение № 1. Опросный лист.

[2] Павлюков В.В. Теоретико-правовые основы получения и проверки компьютерной информации, размещённой на сайтах с ограниченным доступом // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 2 (99). – С. 231.

[3] См.: Приложение № 1. Опросный лист.

случае отсутствия такой возможности владелец хостинга должен немедленно закрыть доступ к ресурсу до получения разрешения правоохранительных органов.

В целях реализация указанной инициативы, необходимо внести дополнения в п.1 ст. 64 ФЗ «О связи», изложив последний в следующей редакции: «1) информация о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи» в текстовом файле на удаленный выделенный сервер МВД для аналитических целей, не нарушающих частную жизнь граждан. На сервер должны передаваться все данные, а отображаться при запросе сотрудника полиции только данные в отношении лиц, которые имеются в банках данных ОВД, а именно накопленные на основании ст. 17 ФЗ «О полиции», с соблюдением установленных законом процедур.

Опрошенные нами сотрудники ОВД подавляющим большинством (79%) поддержали объединение данных и считают необходимым получение и объединение компьютерной информации о гражданах, которые ранее привлекались за преступления и правонарушения из сети Интернет с информацией, которая хранится в банках данных МВД, 5 % с этим не согласны, 16 % воздержались[1].

Касаемо нормативных положений п.2. ст. 64 ФЗ «О связи», хотелось бы указать на то, что последние не целесообразно реализовывать в отношении всех пользователей, а лишь в отношении конкретных лиц, например, как это сделано в США с письмами NSL. То есть, операторы связи обязаны хранить на территории Российской Федерации только «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 основании мотивированного запроса от правоохранительных органов в соответствии с федеральным законодательством». На наш взгляд, это существенно снизит нагрузку на операторов связи.

[1] См.: Приложение № 1. Опросный лист.

В случае отсутствия возможности предоставить такие данные провайдер должен прекратить свою деятельность до полного восстановления механизма передачи LOG-файлов на сервер.

Резюмируя изложенное, отметим, что сегодня ОВД имеют значительный научно-технический потенциал для обработки имеющейся информации с использованием современных средств вычислительной техники, которая позволяет значительно увеличить объем обрабатываемой информации и сократить время поиска необходимых данных. Однако успешная борьба в противодействии преступности в современных условиях невозможна без надлежащего развития информационных систем ОВД, постоянного получения и контроля компьютерной информации. ОВД должны более тщательно систематизировать имеющуюся информацию и обеспечивать доступ к ней оперативных подразделений. В этих целях необходимо создать и законодательно закрепить за каждым подразделением МВД статистический IP- и электронный почтовый адрес, с помощью которого возможно запрашивать дополнительную необходимую информацию у провайдера, владельца интернет-ресурса, принадлежащего Российскому сегменту Интернета.

Также целесообразно создать механизмы объединения как подведомственной, так и неведомственной компьютерной информации, что предоставит возможность сотрудникам полиции оперативно отслеживать и фиксировать противоправную деятельность лица, идентифицировать и предотвращать готовящиеся преступления, а полученные результаты, в рамках ОРМ «Наведение справок», формировать в справку. Благодаря этому также снизится нагрузка на ОВД и повысится авторитет полиции РФ в целом, возникнут дополнительные возможности для оперативного раскрытия и расследования преступлений, установления личности преступника «онлайн» и в режиме реального времени[1].

[1] Павлюков В.В. Оперативное распознавание лица по фото-, видео- и аудиоданным: перспективы внедрения современных технологий в деятельности органов внутренних дел // Вестник Костромской государственный университет имени Н.А. Некрасова. – 2016. – № 6. – С. 206.

ЗАКЛЮЧЕНИЕ

Изучение вопроса, связанного с теоретическими основами и практикой использования компьютерной информации в противодействии преступности, позволило прийти к следующим научно обоснованным выводам:

1. Компьютерная информация – совокупность цифровых данных, имеющих различную форму представления (текстовую, графическую, видео, звуковую, числовую), находящихся на электронных носителях, которые могут быть получены, сохранены, отображены, изменены, закодированы с возможностью дальнейшей передачи при помощи компьютерных устройств и систем в виде электронных, световых, звуковых или радиосигналов.

2. Развитие современных компьютерных технологий способствовало видоизменению работы с информацией. Лица, склонные к занятию противоправной деятельностью, также перенесли свою деятельность в компьютерную сеть. Данный факт свидетельствует о том, что, если сотрудник ОВД будет своевременно получать компьютерную информацию, это позволит оперативно фиксировать и даже выявлять подготовку преступлений.

3. Компьютерная информация, используемая в расследовании преступлений – совокупность актуальных данных, находящихся в компьютере, на компьютерных носителях или передаваемых при помощи компьютерных сетей и систем, имеющих криминалистическое 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.

4. Основными признаками компьютерной информации оперативно-розыскного значения являются трансграничность, относительная неисчерпаемость, измеримость, трансформируемость, защищенность, обезличенность, автоматизация обработки, потенциальная 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.

5. Основное целевое назначение использования компьютеров в том, что компьютерная информация может служить информационной основой для выдвижения версий по делам о преступлениях, совершаемых как в компьютерной сети, так и за ее пределами.

6. Используя информационные технологии, преступник оставляет компьютерные следы на узлах и компьютерных устройствах, периферийных и сетевых устройствах. Файлы с данными (Log-файлы), а также программное обеспечение, которое подвергается преступным посягательствам, становятся носителями следовой информации.

7. Охарактеризованы источники компьютерной информации и классифицированы как:

- По способу передачи: посредством электрических проводов, включая 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-сервера, сервера 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:

- не зашифрованные 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 комбинациий 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 таким относятся как ресурсы сети Интернет с ограниченным доступом, так и компьютерные устройства (стационарные компьютеры, ноутбуки, мобильные телефоны, планшеты, аудио и видео регистраторы, сервера, 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. Подчеркнем, что практически любую компьютерную информацию из открытой можно сделать с ограниченным доступом.

8. В ходе анализа действующего законодательства и зарубежного опыта сделан вывод о том, что многие страны мира взяли на вооружение методы получения и доступа к компьютерной информации в рамках строгого правового регулирования, а иногда и получают доступ к данным путем удаленного доступа и

взлома, что закреплено на законодательном уровне. В свою очередь российский правовой опыт содержит такие нормативные механизмы, которые усложняют процедуру получения оперативно значимых данных из компьютерной сети, из-за чего теряется их оперативность и поэтому стоит частично перенять зарубежный опыт с учетом национальных особенностей и конституционных гарантий. Поэтому, в ФЗ «Об оперативно-розыскной деятельности» нужно закрепить возможность для правоохранительных органов удаленного доступа к компьютерной информации с целью ее оперативного получения при наличии достаточных оснований и соответствующего судебного контроля. В ст. 6 ФЗ «Об оперативно-розыскной деятельности» также следует указать на то, что «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 получать необходимые для выполнения возложенных на оперативные подразделения обязанностей данные у операторов и организаторов распространения информации в сети Интернет путем запроса посредством 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».

9. На основании анализа российского и зарубежного законодательства предложено перечень ОРМ, зафиксированных в ст. 6 ФЗ «Об оперативно-розыскной деятельности», дополнить новым оперативно-розыскным мероприятием – «Компьютерная разведка». Сущность данного ОРМ проявляется в том, что компьютерная информация оперативно-розыскного значения будет получена оперативными сотрудниками России путем санкционированного преодоления компьютерной защиты (проведение SSRF-атаки, SQL-инъекции, использование эксплойтов, поиск RCE-уязвимостей и т. п.) на удаленных интернет-ресурсах или же путем анонимного получения информации от злоумышленников

при помощи сети Интернет в рамках предусмотренных законом процедур.

10. Предложены типовые версии, которые могут применяться следователями при расследовании преступлений, а именно, в зависимости от:

- наличия первично значимой информации в ведомственных и вневедомственных базах данных;

- физического места нахождения информационного источника;

- состояния технического средства, содержащего компьютерную информацию;

- специализации в области информационных технологий владельца информационного источника или пользователя программного обеспечения.

11. Определены основные форм взаимодействия следственных и оперативно-розыскных подразделений с учетом поиска и использования компьютерной информации в расследовании преступлений.

12. При анализе особенностей использования специальных знаний при получении компьютерной информации, обоснован вывод о необходимости задействования специалиста тогда, когда требуются специальные знания в области программирования и при работе со специальным программным обеспечением, а также для криминалистического исследования вещественных доказательств с целью обнаружения, фиксации и изъятия следов преступного поведения лиц, осуществляющих 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, а также задействуя возможности искусственного интеллекта.

13. Также предлагаются авторские тактики, методики и приведены практические примеры по получению компьютерной информации, которая может свидетельствовать о подготовке или совершении преступлений, а именно создание и использование собственного фишингового сайта (при отсутствии признаков провокации) для получения компьютерной информации, использование парсинга и т. д.

14. Возможности компьютерных технологий, в отличие от традиционных способов, позволяют получить и более детально зафиксировать компьютерную информацию, используемую в расследовании преступлений при помощи проведения таких ОРМ, как «Наведение справок», «Снятие информации с технических каналов связи», «Получение компьютерной информации». В последствии данная информация может получить статус доказательства, если она будет надлежащим образом зафиксирована, например, в случае, когда информации будет получена в ходе проведения ОРМ «Получение компьютерной информации», при помощи специализированного программного обеспечения или скриншота, на котором будет отражено кто, где, в какое время и при помощи какого устройства его сделал. 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 дополнительной информации, обеспечивающее ее достоверность и неизменность. Это может способствовать успешному проведению таких следственных действий, как осмотр предмета (документа), выемка, допросы подозреваемого, свидетелей и оперативных сотрудников.

15. В целях обеспечения возможности оперативного получения сотрудниками и подразделениями ОВД компьютерной информации, а также систематизации результатов правоохранительной деятельности обоснована необходимость совмещения данных, накопленных в криминалистических, а также других учетах ОВД, с информацией, которая циркулирует в сети Интернет и хранится у провайдеров и операторов связи.

16. С целью повышения эффективности проведения ОРМ на законодательном уровне также предлагается:

- внести изменения в ФЗ «О связи», а именно в п.1 ст. 64 указать, что «операторы связи и хостинг-провайдеры обязаны в режиме реального времени настроить передачу по защищённым каналам связи Log-файлов, в которых будет записана информация о фактах приема, передачи, доставки и (или) обработки

голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи» в текстовом файле на удаленный выделенный сервер МВД для аналитических целей, не нарушающих частную жизнь граждан. На сервер должны передаваться все данные, а отображаться при запросе сотрудника полиции только данные в отношении лиц, которые имеются в банках данных ОВД, а именно накопленные на основании ст. 17 ФЗ «О полиции», с соблюдением установленных законом процедур.

- указать в п.2. ст. 64 ФЗ «О связи», что, операторы связи обязаны хранить на территории Российской Федерации только «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 на основании мотивированного запроса от правоохранительных органов в соответствии с федеральным законодательством».

17. Необходимо создать специализированный программно-аппаратный комплекс, с помощью которого накопленную информацию в различных неведомственных поисковых системах и социальных сетях объединять с поисковыми программами системы МВД в интегрированные банки данных, стыковка и анализ которых позволит полноценно получать компьютерную информацию и в дальнейшем использовать ее в противодействии преступности.

18. Проанализировав судебную практику, установлено, что фиксация компьютерной информации сотрудниками ОВД осуществляется путем снимка экрана смартфона или монитора компьютера (скриншот) с соблюдением требований к процессуальной форме. Впоследствии составляется акт или протокол ОРМ, к которому прилагаются скриншоты. В протоколе 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.

19. Указано на целесообразность адаптировать искусственный интеллект для

решения специфических криминалистических задач, а именно:

1) для разработки и планирования порядка проведения как одного, так и ряда следственных действий с использованием методической базы по проведению расследования как в целом, так и в частности;

2) для проведения анализа материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера и разработки путей устранения уже имеющихся ошибок и недопущения их в будущем (машинное обучение).

20. Определены тактические особенности использования компьютерной информации при подготовке и осуществлении таких отдельных следственных действий, как осмотр предметов (документов) и допрос. Следователь во время проведения следственных действий может давать поручения оперативному сотруднику по поводу проведения дополнительных мероприятий, направленных на установление мест и времени посещения пользователя, его связей, интересов, комментариев на форумах и блогах, а также поручения по поводу направления запросов владельцам интернет-ресурсов, операторам мобильной связи и интернет-провайдерам на предмет установления сетевой активности пользователя и принадлежности ему определенного оборудования. При этом обосновывается, что компьютерная информация может выступать ориентиром для установления данных о пользователе (ФИО, IP-адрес, e-mail, номер мобильного телефона) и предмета, при помощи которого совершалась противоправная деятельность (мобильный телефон, планшет, стационарный компьютер, сетевое оборудование и т. д.). Тактическим приемом использования компьютерной информации будет демонстрация компьютерной информации при допросе, а именно, процессуально оформленная информация в виде распечатанного скриншота, содержащего сведения о противоправной деятельности, а в случае отрицания принадлежности информации подозреваемому, предъявление справки об активности пользователя от оператора связи, интернет- и хостинг- провайдера, владельца интернет-ресурса, что может указывать не только на осведомленность об обстоятельствах, имеющих отношение к расследуемому событию, но также и на то, что эта информация уже

закреплена как доказательство.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

2. О полиции: Федеральный закон от 07 февраля 2011 № 3-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

3. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

4. Об оперативно-розыскной деятельности: Модельный закон (новая редакция) [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/902050857 (дата обращения: 15.01.2025).

5. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» Федеральный закон Российской Федерации от 01 мая 2019 № 90-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

6. О внешней разведке: Федеральный закон от 10 января 1996 N 5-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

7. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 23.01.2025).

8. О Федеральной службе безопасности: Федеральный закон от 03 апреля 1995 № 40-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 19.01.2025).

9. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 11.01.2025).

10. О связи: Федеральный закон от 07 июля 2003 № 126-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.01.2025).

11. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.01.2025).

12. Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 15.02.2025).

13. Уголовно-процессуальный кодекс РФ от 18 декабря 2001 № 174-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

14. О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Федеральный закон от 01 октября 2008 № 164-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 22.02.2025).

15. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06 июля 2016 № 375-ФЗ [Электронный

ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

16. 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»: Федеральный закон от 06 июля 2016 № 374-ФЗ [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 13.02.2025).

17. Об особенностях использования национального сегмента сети Интернет: Указ Президента Республики Беларусь от 18 сентября 2019 г. № 350 [Электронный ресурс] // Официальный Интернет-портал Президента Республики Беларусь. – URL: http://president.gov.by/uploads/documents/2019/350uk.pdf (дата обращения: 14.02.2025).

18. Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий: Приказ Министерства информационных технологий и связи Российской Федерации от 16 января 2008 г. № 6 [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102094659&backlink=1&&nd=102120563 (дата обращения: 12.02.2025).

19. Об утверждении инструкции по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений: Приказ МВД от 20 июня 1996 г. № 334. Утратил силу в связи с изданием Приказа МВД РФ от 26.03.2008 № 280дсп. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=390400#09107784133705303 (дата обращения: 27.02.2025).

20. Об утверждении устава федерального казенного учреждения «Главный информационно-аналитический центр министерства внутренних дел Российской Федерации: Приказ МВД России от 31 декабря 2010 № 910 [Электронный ресурс] // Официальный сайт МВД РФ. – URL: https://mvd.ru/upload/site1/folder_page/006/825/743/Prikaz_910-GIATs.doc (дата

обращения: 26.02.2025).

21. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 [Электронный ресурс] // Справочно-правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_155629/ (дата обращения: 19.02.2025).

22. О печатных средствах массовой информации (печати) в Украине: Закон Украины № 2782-XII от 16 ноября 1992 [Электронный ресурс] // Официальный сайт Верховной Рады Украины. – URL: http://zakon3.rada.gov.ua/laws/show/2782-12 (дата обращения: 11.02.2025).

23. Об оперативно-розыскной деятельности: Закон Украины от 18 февраля 1992 года № 2135-XII [Электронный ресурс] // Официальный сайт Верховной Рады Украины – URL: http://zakon2.rada.gov.ua/laws/show/2135-12/page2 (дата обращения: 11.02.2025).

24. О телекоммуникациях: Закон Украины от 18 ноября 2003 № 1280-IV [Электронный ресурс] // Официальный сайт Верховной Рады Украины. – URL: http://www.Zakon.rada.gov.ua (дата обращения: 11.02.2025).

25. Письмо Федеральной налоговой службы от 31 марта 2016 г. № СА-4-7/5589 О понятии «скриншот» («снимок экрана») и порядке его использования. [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71284846/ (дата обращения: 04.03.2025).

26. Конвенция о киберпреступности (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года [Электронный ресурс]. – URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения: 01.02.2025).

27. ISO/IEC 2382:2015, Information technology – Vocabulary – Part 1: Fundamental terms: a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or communication, or processing

[Электронный ресурс]. – URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (дата обращения: 01.02.2025).

28. Regulation of Investigatory Powers Act 2000 [Электронный ресурс]. – URL: https://www.legislation.gov.uk/ukpga/2000/23/contents (дата обращения: 08.02.2025).

29. Bill proposes ISPs, Wi-Fi keep logs for police [Электронный ресурс]. – URL: http://edition.cnn.com/2009/TECH/02/20/internet.records.bill/index.html (дата обращения: 08.02.2025).

30. Broadcasting Services Amendment (Online Services) Act 1999 16.07.1999 No. 90 [Электронный ресурс]. – URL: https://www.legislation.gov.au/Details/C2004A00484 (дата обращения: 08.02.2025).

31. Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) [Электронный ресурс]. – URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=2445#FN501 (дата обращения: 09.02.2025).

32. Directive 2006/24/EC of the European parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [Электронный ресурс]. – URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (дата обращения: 15.02.2025).

33. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Электронный ресурс]. – URL: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (дата обращения: 16.02.2025).

34. Computer crime act of 1978 [Электронный ресурс]. – URL: http://docweb.cns.ufl.edu/docs/d0010/d0010.html (дата обращения: 13.02.2025).

35. Press release extraordinary council meeting justice and home affairs Brussels, 13 July 2005 [Электронный ресурс]. – URL: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf (дата обращения: 13.02.2025).

36. 18 U.S. Code § 2704 – Backup preservation [Электронный ресурс]. – URL: https://www.law.cornell.edu/uscode/text/18/2704 (дата обращения: 13.02.2025).

37. Protection of Children Act 1978 [Электронный ресурс]. – URL: https://www.legislation.gov.uk/ukpga/1978/37 (дата обращения: 14.02.2025).

38. German Data Retention Act Signed Into Law [Электронный ресурс]. – URL: http://www.winston.com/en/privacy-law-corner/new-german-data-retention-law-expected-to-take-effect-soon.html (дата обращения: 14.02.2025).

39. USA Patriot Act (H.R. 3162) https://epic.org/privacy/terrorism/hr3162.html (дата обращения: 09.02.2025).

40. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 [Электронный ресурс]. – URL: https://www.legislation.gov.au/Details/C2015A00039 (дата обращения: 13.02.2025).

41. Surveillance devices act № 64 of 2007 [Электронный ресурс]. – URL: http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/sda2007210/ (дата обращения: 14.02.2025).

Материалы судебной практики:

42. German court orders stored telecoms data deletion [Электронный ресурс] News BBC. – URL: http://nzsxo4y.mjrgg.mnxs45ll.cmle.ru/2/hi/europe/8545772.stm (дата обращения: 22.02.2025).

43. European Court of Justice Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014 [Электронный ресурс]. – URL: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN (дата обращения: 22.02.2025).

44. Определение Конституционного Суда РФ от 27.02.2018 № 328-О Об отказе в принятии к рассмотрению жалобы гражданина Рачкова Станислава Евгеньевича на нарушение его конституционных прав статьями 6, 7 и 8, пунктом 1

части первой статьи 15 Федерального закона «Об оперативно-розыскной деятельности». – URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-27022018-n-328-o/ (дата обращения 08.02.2025).

45. Приговор Сакмарского районного суда Оренбургской области № 1[1]-21/2017 от 25 июля 2017 г. [Электронный ресурс]. – URL: http://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/28593136 (дата обращения: 08.02.2025).

46. Приговор Останкинского районного суда по ч. 3 ст. 228.1 УК РФ № 1-278/2015 [Электронный ресурс]. – URL: http://www.sud-praktika.ru/precedent/82963.html (дата обращения: 08.02.2025).

47. Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-322/2017 от 9 ноября 2017 г. по делу № 1-322/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/5RIILb1PXPUz/ (дата обращения: 08.02.2025).

48. Приговор Лесосибирского городского суда (Красноярский край) № 1-275/2018 от 18 октября 2018 г. по делу № 1-275/2018 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/YXnsYURSnoJL/ (дата обращения: 09.02.2025).

49. Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-164/2017 от 18 августа 2017 г. по делу № 1-164/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TweV9tbuut5Z/ (дата обращения: 09.02.2025).

50. Приговор Приморского районного суда г. Новороссийска (Краснодарский край) № 1-458/2017 1-63/2018 от 2 февраля 2018 г. по делу № 1-458/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/gaRcTHh7C6dC/ (дата обращения: 09.02.2025).

51. Приговор Приморского районного суда г. Новороссийска (Краснодарский край) № 1-130/2017 от 17 мая 2017 г. по делу № 1-130/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/GPSNpiTKsHYB/ (дата обращения: 09.02.2025).

52. Приговор Октябрьского районного суда г. Новороссийска (Краснодарский край) № 1-244/2017 от 17 ноября 2017 г. по делу № 1-244/2017

[Электронный ресурс]. – URL: https://sudact.ru/regular/doc/QODcLxpWm5dr/ (дата обращения: 10.02.2025).

53. Приговор Фрунзенского районного суда г. Владимира, Владимирская область, Российской Федерации. - № 1-86/2018 от 24 сентября 2018 г. по делу № 1-86/2018 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TqnXFydxjZx4/ (дата обращения: 10.02.2025).

54. Постановление Анапского городского суда (Краснодарский край) № 5-3613/2018 от 2 ноября 2018 г. по делу № 5-3613/2018[Электронный ресурс]. – URL: https://sudact.ru/regular/doc/iD75SkvOV7by/ (дата обращения: 11.02.2025).

55. Постановление Приморского районного суда г. Новороссийска (Краснодарский край) № 5-89/2017 от 18 января 2017 г. по делу № 5-89/2017 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/oAodNVevI8Nh/ (дата обращения: 11.02.2025).

56. Решение Абинского районного суда (Краснодарский край) № 12-40/2018 от 25 мая 2018 г. по делу № 12-40/2018[Электронный ресурс]. – URL: https://sudact.ru/regular/doc/6YL6sesUHsHt/ (дата обращения: 12.02.2025).

Учебники, учебные пособия и монографии:

57. Бобров В.Г. Понятие оперативно-розыскных мероприятий. Основания и условия проведения оперативно-розыскных мероприятий: Лекция. – М.: Академия управления МВД России. – 2003. – С. 23-24.

58. Белкин Р.С. Криминалистическая энциклопедия. М.: Издательство Бек, 1997. – 342 с.

59. Белкин Р.С. Криминалистическая энциклопедия. – М.: Мегатрон XXI, 2000. – 2-е изд. доп. – 334 с.

60. Белкин А.Р. Теория доказывания. Научно-методическое пособие. – М. : Издательство НОРМА, 1999. – 429 с.

61. Гайдин А. И. Особенности взаимодействия следователя с должностными лицами правоохранительных органов при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Вестник Воронежского института МВД России. – 2020. – №. 3. – С. 177-183.

62. Головин М. В. Проблемы целеопределения в расследовании: монография / М. В. Головин, Н. М. Шпак. – Краснодар: КубГАУ, 2014. – 162 с.

63. Данильян С.А. Взаимодействие органов правоохранительных систем. Монография / С.А. Данильян. – Краснодар: КубГАУ. – 2016. – 118 с.

64. Карпова И.П. Базы данных: учебное пособие. - СПБ.: Питер, 2013. – 240 с.

65. Крылов В.В. Расследование преступлений в сфере информации. - М.: Издательство «Городец», 1998. – 264 с.

66. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В.Б. Вехов. – Волгоград: ВА МВД России, 2008. – 407 с.

67. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.

68. Дубягин Ю.П., Дубягина О.П., Михайлычев Е.А. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» (постатейный). [Электронный ресурс]. – URL: https://www.lawmix.ru/commlaw/1518 (дата обращения: 24.02.2025).

69. Дуленко В.А., Бронфман Б.Е. К вопросу расследования преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. – 2016. – № 2 (72). – С. 45-49.

70. Зеленский В.Д. Организационные функции субъектов расследования преступлений: монография / В.Д. Зеленский. – Краснодар: КубГАУ, 2005. – 193 с.

71. Зеленский В.Д. О понятии и содержании организации расследования преступлений // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9, № 4. – С. 734–744.

72. Зеленский В.Д. Теоретические вопросы организации расследования преступлений. Монография. – Краснодар: КубГАУ, 2011. – 156 с.

73. Криминалистика: учебник для вузов / Под ред. Р.С. Белкина. – М. :

НОРМА, 2001. – 990 с.

74. Криминалистика: учебник / под ред. д.ю.н., профессора В.Д. Зеленского и д.ю.н., профессора Г.М. Меретукова – СПб, Издательство «Юридический центр», 2015. – 704 с.

75. Криминалистика: учебник / под. ред. Е.П. Ищенко. – М.: Проспект, 2011. – 504 с.

76. Овчинский А.С. Информация и оперативно-розыскная деятельность: Монография / Под ред. заслуженного юриста Российской Федерации, доктора юридических наук, профессора В.И. Попова. – М.: ИНФРА-М, 2002. – 97 с.

77. Оперативно-розыскная деятельность органов внутренних дел. Термины и определения: Учебное пособие / Под ред. Ю.И. Римаренко. – Киев: НИиРИО КВШ МВД СССР, 1988. – 311 с.

78. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений // Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., дополненное. – М.: ООО «А ТЕМП», 2006. – 944 с.

79. Посков Я.А. Роль единой информационно-телекоммуникационной системы органов внутренних дел в информационном обеспечении производства следственных действий // Известия Тульского государственного университета. Экономические и юридические науки. – 2009. – №. 1. – С. 338-342.

80. Пристансков В.Д., Харатишвили А.Г., Евстратова Ю.А. Искусственный интеллект - новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений // Всероссийский криминологический журнал. – 2023. – Т. 17. – № 6. – С. 586-596.

81. Решняк О.А. Расследование преступлений в сфере незаконного сбыта опасных психотропных веществ, совершенных с использованием компьютерных технологий: монография / О.А. Решняк, С.А. Ковалев, В.Б. Вехов. – Волгоград: ВА МВД России, 2020. – 192 с.

82. Современное оружие сотрудников органов внутренних дел: информационные технологии как ответ на вызов времени: практ. пос. /

Ю.А. Задорожний, А.Е. Трубкович, О.В. Колтырин, и др. / МВД Украины, Луганский государственный университет внутренних дел им. Э.А. Дидоренко. – Луганск: РИО ЛГУВД им. Э.А. Дидоренко, 2012. – 64 с.

83. Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – М.: ИНФРА-М, 2006. – 832 с.

84. Ткалич В.Л., Лабковская Р.Я., Пирожникова О.И., Коробейников А.Г., Симоненко З.Г., Монахов Ю.С. Патентоведение и защита интеллектуальной собственности. Учебное пособие. – СПб: Университет ИТМО, 2015. – 171 с.

85. Яблоков Н.П. Криминалистика. 2-е изд. перераб и доп. М.: Юрайт, 2014. – 303 с.

Научные статьи:

86. Алавердов О.С. Международное сотрудничество в области борьбы с Интернет-преступностью // Общество и право. – 2010. – № 3(30). – С. 165-168.

87. Александров И.В. Проблемные аспекты формирования методики расследования современных преступлений, совершаемых в сфере экономики // Вестник Московского университета. Серия 11: право – 2014. – № 4. – С. 34-42.

88. Алиева Г.А., Кустов А.М. Получение криминалистически значимой информации из мессенджера Whatsapp в качестве источника доказательственной информации // в книге: Проблемы получения и использования доказательственной и криминалистически значимой информации. материалы Международной научно-практической конференции. – 2019. – С. 3-4.

89. Алиуллов Р.Р., Саетгараев В.Ф. Сущность и основные принципы взаимодействия подразделений полиции в сфере реализации оперативно-служебных задач // Вестник Казанского юридического института МВД России. – 2015. – № 2(20). – С. 70-75.

90. Алябьев А.А., Лагуточкин А.В. Проблемы осуществления оперативно-розыскных мероприятий в информационном пространстве сети Интернет // Проблемы правоохранительной деятельности. – 2013. – № 1. – С. 66-69.

91. Антонов И.Ю. Некоторые направления совершенствования оперативно-розыскного мероприятия «Наблюдение», проводимого с применением

технических средств // Общество и право. – 2015. – № 2(52). – С. 217-219.

92. Архипов А.Ю. Основные направления и проблемные вопросы использования банков данных видеоинформации в деятельности оперативных подразделений при раскрытии преступлений // Вестник Нижегородской академии МВД России. – 2015. – № 1(29). – С. 213-217.

93. Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. – 2017. – № 2(65). – С. 31-33.

94. Баринов С.В. Следы преступных нарушений неприкосновенности частной жизни как элемент криминалистической характеристики / Вестник Удмуртского университета. серия экономика и право Издательство: Удмуртский государственный университет (Ижевск). – 2016. – № 1(26). – С. 85-90.

95. Батоев В.Б. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет // Вестник ВИ МВД России. – 2016. – № 2. – С. 37-43.

96. Бахтеев Д.В. О некоторых способах сокрытия и обнаружения компьютерной информации // Сборник материалов криминалистических чтений. – 2017. – № 14. – С. 18-19.

97. Берова Д.М., Тутуков А.Ю. Потенциал искусственного интеллекта в расследовании преступлений: за или против // Социально-политические науки. – 2024. – Т. 14. – № 3. – С. 96-100.

98. Беспалова Е.В. Киберпреступность: история уголовно–правового противодействия // Информационное право. – 2006. – № 4(7). – С. 3-5.

99. Бирюков Д.В. Компьютерная информация как предмет преступного посягательства [Электронный ресурс]. – URL: http://aspirantura.16mb.com/doc/conf2015/s3/Biryuk.doc (дата обращения: 20.02.2025).

100. Боканов А.А. Понятие информации в современной экономической науке // Армия и общество. – 2010. – № 1. – С. 120-126.

101. Борисенко А.А. О сущности информации // Фундаментальные

исследования. – 2005. – № 7 / [Электронный ресурс]. – URL: https://www.fundamental-research.ru/ru/article/view?id=6331 (дата обращения: 18.02.2025).

102. Борисов В.В. Об особенностях фиксации информационных следов в практике защиты информации // Известия ЮФУ. Технические науки. – 2009. – № 5. – С. 164-168.

103. Бородин В.С. Системный подход к организации взаимодействия органов досудебного следствия и дознания // Ученые записки Таврического национального университета имени В.И. Вернадского. Серия: Юридические науки. – 2011. – Т. 24. – № 2 (63). – С. 237-245.

104. Бурцева Е.В., Рак И.П., Селезнев А.В., Терехов А.В. Роль информационных технологий в профилактике и раскрытии преступлений // Вестник ТГУ. – 2008. – № 2. – С. 479-482.

105. Бусов А.В. Использование габитоскопических учётов в раскрытии, расследовании и предупреждении преступлений // Вестник Санкт-Петербургского университета МВД России. – 2011. – № 4. – С. 77-81.

106. Васюков В.Ф. Осмотр, выемка электронных сообщение и получение компьютерной информации // Уголовный процесс. – 2016. – № 10. – С. 64-67.

107. Вахрушев С.Ю., Дмитриева А.А. Прослушивание телефонных переговоров как разведывательное оперативно-техническое мероприятие // Вестник ЮУрГУ. Серия: Право. – 2006. – № 13. – С. 35-38.

108. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 209-216.

109. Власов М.П., Голоскоков К.П., Черкова М.Ю. Технологии научных исследований в «сети корпоративных знаний» // Сборник научных трудов SWorld: Материалы международной научно-практической конференции «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании 2012». – Одесса: Куприенко, 2012. – № 4(30). – С. 5-13.

110. Волеводз А.Г. Следы преступлений, совершенных в компьютерных

сетях // Российский следователь. – 2002. – № 1. – С. 4-12.

111. Воронкова Д.К., Манучарян А.К. Осмотр и судебная экспертиза мобильного устройства в рамках расследований по уголовным делам // Международный журнал гуманитарных и естественных наук. – 2019. № 7-2. – С. 119-120.

112. Воронов И.А. Зарубежный опыт борьбы с киберпреступностью [Электронный ресурс]. – URL: http://www.crime-research.ru (дата обращения: 19.01.2025).

113. Грицаев С.И., Помазанов В.В., Заболотняя Ю.А. Компьютеризация целеопределения и планирования расследования // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2015. – № 108. [Электронный ресурс]. – URL: http://ej.kubagro.ru/2015/04/pdf/36.pdf (дата обращения: 25.01.2025).

114. Гришин Ю.В., Иванов А.В., Карпова Н.Е., Чуваков А.В. Применение автоматизированных систем в компьютерной криминалистике // Безопасность цифровых технологий. – 2022. – № 2 (105). – С. 21-33.

115. Давыдов В.О., Головин А.Ю., Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия тульского государственного университета. экономические и юридические науки. – Тула: Издательство Тульского государственного университета. – 2016. – № 3-2. – С. 254-259.

116. Демина Р.Е. Информационное обеспечение раскрытия преступлений: пути оптимизации // Вестник Поволжской академии государственной службы. – 2008. – № 3. – С. 83-87.

117. Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. Вопросы студенческой науки. – 2017. – № 15. – С. 179-183.

118. Добренко М.А. Возможности использования результатов оперативно-розыскного мероприятия «Опрос» в уголовном процессе // Историческая и социально-образовательная мысль. – 2015. – № 3(7). – С. 108-110.

119. Домашенко И.Е. Тактика подготовительной части допроса по преступлениям в сфере компьютерной информации // Ломоносовские чтения на Алтае: фундаментальные проблемы науки и образования. – 2015. – С. 3073-3075.

120. 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.

121. Дунаева М.С. Проблемы защиты частной жизни граждан при осуществлении контроля и записи переговоров // Адвокатская практика. – 2003. – № 3. – С. 13-17.

122. Дытченко Г.В., Никитин Е.Л. Законность проведения оперативно-розыскных мероприятий, ограничивающих конституционные права граждан // Криминалист. – 2011. – № 1(8). – С. 101-108.

123. Евтеев С.П. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Общедоступная информация и информация ограниченного доступа, информационно-телекоммуникационная сеть интернет, осмотр и выемка компьютерной информации / Вестник всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2017. – № 1(41). – С. 42-50.

124. Емельянов С.Л. Техническая разведка и технические каналы утечки информации // Одесская национальная юридическая академия. – 2010. – № 3(84). – С. 20-23.

125. Еремченко В.И., Зиновьева Н.С. Алгоритм использования электронного почтового ресурса как источника доказательственной информации // Вестник Краснодарского университета МВД России. – 2014. – № 3 (25). – С. 62-65.

126. Еськов В.Д., Чеботарев С.А. Особенности осмотра страниц в сети интернет // В сборнике: организационное, процессуальное и криминалистическое обеспечение уголовного производства Материалы VI Международной научной конференции студентов и магистрантов. – 2017. – С. 39-40.

127. Ефимкина Н.В. К вопросу об искажении информации в деятельности сотрудников органов внутренних дел // Психопедагогика в правоохранительных

органах. – 2013. – № 4(55). – С. 16-18.

128. Ефремов К.А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. – 2016. – № 6. – С. 92-95.

129. Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник Удмуртского университета. Серия Экономика и право. – 2011. – № 4. – С. 114-118.

130. Журавленко Н.И., Шведова Л.Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. – 2015. – № 3(53). – С. 66-70.

131. Законодательство об оперативно-розыскной деятельности отстает от жизни: интервью с Сергеем Викторовичем Ивановым, начальником управления по надзору за производством дознания и оперативно-розыскной деятельностью Генеральной прокуратуры РФ // Уголовный процесс. 2016. № 3. – С. 24-33.

132. Зверянская Л.П. Дискуссионные проблемы выявления и предупреждения киберпреступлений // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 8. – С. 160-161.

133. Зеленский В.Д., Агеев Н.В. О структуре организационного процесса отдельного расследования // Вестник Самарского юридического института. – 2019. – № 3 (34). – С. 42-45.

134. Зигмунт О.А., Петровский А.В. Кибер и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. – 2015. – № 4(34). – С. 180-188.

135. Зиновьева Е.С. Развитие информационного общества: проблемы безопасности // Вестник МГИМО. – 2012. – № 1. – С. 130-135.

136. Игнатенко Л.Н. Организационно-тактические особенности проведения обыска по компьютерным преступлениям // Российский государственный педагогический университет им. А.И. Герцена. – 2016. – № 10(12). – С. 49-52.

137. Индрисова З.Н. Отсутствие законодательного закрепления терминов

«Информация» и «Компьютерная информация» как проблема выявления стратегий по борьбе с компьютерной преступностью в Российской федерации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) Краснодар: КубГАУ, 2014. – № 99(5). [Электронный ресурс]. – URL: http://ej.kubagro.ru/2014/05/pdf/88.pdf (дата обращения: 22.01.2025).

138. Исакова А.Г., Осин А.В. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «Дипфейк» // Вестник науки. – 2024. – Т. 3. – № 1 (70). – С. 235-242.

139. Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. – С. 116-123.

140. Казанцев С.Я., Згадзай О.Э. Экономическая преступность в IT-сфере. Новые угрозы и необходимые ответы // Вестник Казанского юридического института МВД России. – 2011. – № 3. – С. 30-36.

141. Карагодин В.Н., Костомаров К.В. Проблемы установления субъекта незаконного доступа к компьютерной информации банков // Библиотека криминалиста. Научный журнал. – М. 2013. – № 5(10). – С. 193-201.

142. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46-50.

143. Карпычев В.Ю., Немкова Н.А. Мировой опыт правового регулирования оперативных мероприятий на сетях связи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2010. – № 2(13). – С. 172-174.

144. Ковалев С.И., Иванская А.В. Проблемы правовой защиты информации приватного характера в условиях развития научно-технического прогресса // Вестник РУДН. Серия: Юридические науки. – 2014. – № 1. – С. 44-52.

145. Козаченко И.П. К вопросу об информационном обеспечении оперативно-розыскной деятельности органов внутренних дел // Актуальные

вопросы получения, оценки и использования информации в оперативно-розыскной деятельности органов внутренних дел. – Киев: НИиРИО КВШ МВД СССР, 1986. – С. 3-7.

146. Колесников А.В. Использование результатов оперативно-розыскной деятельности при выявлении и расследовании преступлений против личности // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2016. – № 1. – С. 79-92.

147. Коликов Н.Л. Причины и условия профессиональной компьютерной преступности // Вестник ЮУрГУ. Серия: Право. – 2011. – № 19(236). – С. 30-33.

148. Комаров И.М. «Цифровая криминалистика» – давно назревшая проблема // Библиотека криминалиста. Научный журнал. – 2018. – № 2(37). – С. 154-167.

149. Коровин С.В. Взаимодействие сотрудников оперативных аппаратов и органов предварительного следствия в расследовании и раскрытии бандитизма (методические рекомендации). Тюмень. – 2007. – 29 с.

150. Корчагин А.А., Кобзев И.В. Информационно-программное обеспечение доследственных, следственных и судебных ситуаций по уголовным делам об убийствах // Известия АлтГУ. – 2015. – № 2(86). – С. 73-77.

151. Костякова Н.В. Проблемы отыскания и изъятия виртуальных следов преступлений против половой неприкосновенности несовершеннолетних, совершенных с использованием сети интернет и мобильной связи // Вестник Барнаульского юридического института МВД России. – 2016. – № 2(31). – С. 126-128.

152. Красненко Ю.В. Поисково-познавательная деятельность на первоначальном этапе расследования // Вестник Белгородского юридического института МВД России. – 2019. – №. 3. – С. 52-57.

153. Кремлев М.В. К вопросу о понятии информации, используемой в ходе расследования преступлений // Человек: преступление и наказание. – 2014. – № 4 (87). – С. 101-104.

154. Кругликов А.П. О понятии и системе форм взаимодействия

следователей и органов дознания в процессе расследования и раскрытия преступлений // Успехи современной науки. – 2017. – № 3. – С. 192-194.

155. Кручинина Н.В., Туренко Н.С. Выдвижение и проверка версий // Законность. – 2006. – № 12 (866). – С. 33-34.

156. Куватов В.И., Примакин А.И., Якушев Д.И. Противодействие террористическим и экстремистским организациям в сети Интернет // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 1 (65). – С. 91-94.

157. Кузченко Д.В., Кушпель Е.В. О некоторых тактических особенностях поиска, фиксации и изъятия компьютерной информации в ходе наложения ареста на почтовотелеграфные отправления и при контроле и записи переговоров // Вестник Барнаульского юридического института МВД России. – 2011. – № 1 (20). – С. 39-41.

158. Кузнецов А.А., Муленков Д.В. Тактические и технические аспекты работы с цифровыми средствами фиксации при проведении оперативно-розыскных мероприятий // Юридическая наука и правоохранительная практика, – 2009. – №. 1 (7). – С. 48-59.

159. Куликов А.Г., Лазаревич В.В. О понятии и классификации способов совершения цифровых преступлений // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 1 (15). – С. 68-79.

160. Курьянова Ю.Ю. К вопросу о понятии планирования расследования преступлений // Сибирский юридический вестник. – 2010. – №. 1. – С. 67-71.

161. Кучин О.С. Средства и орудия как элемент механизма преступной деятельности экстремистского характера // Известия Тульского государственного университета. экономические и юридические науки. – 2017. – № 4-2. – С. 45-49.

162. Кучина Я.О. Облачные технологии: понятие и основы правового регулирования // Дальневосточный федеральный университет. – Владивосток. – 2016. – № 4. – С. 77-89.

163. Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Russian journal of criminology. – 2020. –Т. 14. – № 6. – 882-890.

164. Левченкова В.А. Современные научные подходы к формированию учения о виртуальных следах // Сборник материалов III Международной студенческой научно-практической конференции «Уголовно-процессуальный кодекс Российской Федерации: достижения и проблемы применения». – Курск. – 2016. – С. 105-108.

165. Летёлкин Н.В. Особенности уголовно-правового противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») в законодательстве стран англосаксонской правовой семьи (на примере Великобритании и США) // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 2(34). – С. 305-310.

166. Лукашов В.А. О сущности и значении оперативно-розыскной информации // Информационное сообщение лаборатории проблем оперативно-розыскной работы. – М.: НИиРИО ВШ МВД СССР. – 1973. – № 3. – С. 21-22.

167. Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. – 2010. – № 11(167). – С. 18-28.

168. Манукян А.В. Виртуальные следы реальных преступлений // Мир юридической науки. – Санкт-Петербург. – 2015. – № 3. – С. 67-69.

169. Маркелов М.В., Фролов В.Ю. Основные элементы организации оперативно-розыскной деятельности органов внутренних дел // Актуальные проблемы теории оперативно-розыскной деятельности. – Омск: НИиРИО Омской ВШ МВД СССР, 1986. – С. 88-101.

170. Маруев А.Ю. Информационная безопасность России и основы организации информационного противоборства // Проблемный анализ и государственно-управленческое проектирование. – 2010. – № 1. – С. 47-54.

171. Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. – 2014. – № 1(31). – С. 114-121.

172. Махтаев М.Ш., Лебедь И.Е. Криминалистические аспекты предупреждения преступлений в сфере компьютерной информации // Вестник

Российского нового университета. Серия: Человек и общество. – 2009. – № 4. – С. 28-33.

173. Меретуков Г.М., Лунина Е.С., Липка А.О. Сущность и значение поисковой деятельности подразделений, осуществляющих оперативно-розыскную деятельность // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2016. – № 116. – С. 957-976.

174. Митин Е.В. Право на тайну сообщений, передаваемых по электронным почтовым ящикам: проблемы реализации // Теория и практика общественного развития. – 2012. – № 9. – С. 271-273.

175. Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. – 2010. – № 2. – С. 206-209.

176. Меньшова П.Э. К вопросу о нормативном регулировании и применении оперативно-разыскного мероприятия «Получение компьютерной информации» // Научно-методический электронный журнал «Концепт». – 2017. – № 39. – С. 876–880.

177. Мовчан А.В. Отдельные аспекты применения компьютерной разведки в оперативно-розыскной деятельности // Проблемы правоохранительной деятельности. – 2014. – № 2. – С. 107-112.

178. Можаева И.П. Криминалистическое учение об организации расследования преступлений: современное состояние и перспективы // Труды Академии управления МВД России. – 2015. – №. 4 (36). – С. 81-85.

179. Нагорняк Р.В. Получение компьютерной информации: содержание и разграничение с другими оперативно-розыскными мероприятиями // современность в творчестве начинающего исследователя Сборник материалов Всероссийской научно-практической конференции молодых учёных. – 2017. – С. 161-164.

180. Немкова Н.А. Особенности правового регулирования оперативно-розыскных мероприятий в сетях связи // Проблемы правоохранительной деятельности. – 2009. – № 1-2. – С. 68-71.

181. Нестеров А.В. Интернет-поле VS киберпространства // Вопросы безопасности. – 2015. – № 4. – С. 13-27.

182. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55.

183. Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник ВИ МВД России. – 2016. – № 3. – С. 83-90.

184. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 13-19.

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

186. Павлюков В.В. Организационно-правовые основы противодействия кибератакам на инфраструктуру государства // Вестник Московского университета. Серия 11: Право. – 2019. – № 4. – С. 119-128.

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

188. Павлюков В.В. Правовые и организационные основы использования единой информационно-аналитической системы в ОВД // Вестник Костромского государственного университета имени Н.А. Некрасова. – 2017. – № 3. – С. 273-275.

189. Павлюков В.В. Перспективы использования полицией ЛНР современных информационных технологий в противодействии преступности // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2016. – № 1. – С. 260-271.

190. Павлюков В.В. Компьютерная разведка как оперативно-розыскное мероприятие // Вестник Нижегородской академии МВД России. – 2016. – № 4(36).

– С. 236-241.

191. Павлюков В.В. Оперативное распознавание лица по фото-, видео- и аудиоданным: перспективы внедрения современных технологий в деятельности органов внутренних дел // Вестник Костромской государственный университет имени Н.А. Некрасова. – 2016. – № 6. – С. 203-206.

192. Павлюков В.В. Правовая и практическая возможность объединения данных в информационно-поисковых системах МВД РФ с информацией из сети Интернет // Вестник Костромского ГУ им. Н.А. Некрасова МВД России. – 2016. – № 3. – С. 226-229.

193. Павлюков В.В. Некоторые методики раскрытия и расследования преступлений с использованием информационно-поисковых систем ОВД и компьютерной информации из сети интернет // Вестник Луганской академии внутренних дел имени Э.А. Дидоренко. – 2017. – № 2. – С. 161-173.

194. Павлюков В.В. Практические способы получения и использования результатов оперативно-розыскного мероприятия «Получение компьютерной информации» // Вестник Костромского государственного университета. – 2020. Т. 26. – № 3. – С. 199-203.

195. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2015. – № 110. – С. 866-894.

196. Пастухов П.С. Правовые аспекты использования информационных технологий для обеспечения общественной безопасности и общественного порядка // Вестник Прикамского социального института. – 2016. – № 3(75). – С. 6-12.

197. Пахомова В.А. Понятие термина «Информация» и его историческое развитие // Вестник ЮУрГУ. Серия: Право. – 2013. – № 4. – С. 59-64.

198. Пацкевич А.П. Организация расследования преступлений: проблемы, перспективы, тенденции // Вестник Полоцкого государственного университета. – 2011. Серия D. – С. 136-137.

199. Платёнкин А.В. Особенности использования электронных

доказательств при проведении допроса подозреваемого // World science, – 2016. – № 5 (9). – С. 9-11.

200. Попов К.И. Компьютерные преступления – преступления мирового масштаба // Правопорядок: история, теория, практика. – 2013. – № 1(1). – С. 28-31.

201. Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10. – С. 90-96.

202. Просина А.И. Соблюдение статьи 51 Конституции Российской Федерации при проведении допроса: история и современность // Наука. Общество. Государство. – 2018. – № 4 (24). – С. 5-11.

203. Пущин В.С. Преступления в сфере компьютерной информации. – М., 2000. [Электронный ресурс]. URL: https://ndki.narod.ru/liblary/articles/komp_prest/Puschin_VS-Komp_prest1.doc (дата обращения: 17.06.2024).

204. Россинская Е.Р., Семикаленова А.И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. – 2020. – Т. 11. – № 3. – С. 745-759.

205. Россинский С.Б. Проблема использования в уголовном процессе результатов оперативно-розыскной деятельности требует окончательного разрешения // Lex Russica, 2018. №. – 10 (143). – С. 70-84.

206. Рыжов Р.С. Сравнительно-правовой анализ отдельных положений федеральных законов об информации 1995 и 2006 гг, // Вестник ВИ МВД России. – 2011. – № 4. – С. 148-153.

207. Садыков А.У. Использование результатов оперативно-розыскной деятельности при подготовке и проведении допросов // Общество и право. – 2015. – № 3 (53). – С. 193-196.

208. Садырова М.С., Менжега М.М. Осмотр электронных устройств как самостоятельное следственное действие // Юридические науки: проблемы и

перспективы: материалы IV Междунар. науч. конф. – Казань: Изд-во «Бук», 2016. – С. 279-281.

209. Саенко С.И., Павлюков В.В. Правовые, организационные и технологические способы обеспечения кибербезопасности на земле и в космосе // Охрана, безопасность, связь. – 2023. – № 8-1. – С. 100-106.

210. Самитов Э.О., Казанцев С.Я. Типичные версии и планирование расследования истязаний // Вестник Московского университета МВД России, 2016. – №. 4. – С. 209-214.

211. Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. – 2004. – № 1. – С. 53-55.

212. Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. – М.: Теис, 1996. – 704 с.

213. Скоморохов О.Н., Чиненов Е.В. Особенности криминалистической характеристики заведомо ложного сообщения об акте терроризма посредством сети Интернет // Проблемы правоохранительной деятельности. – 2013. – № 1. – С. 61-66.

214. Скурихина А.А., Ронжина О.С. Виктимность в сфере компьютерных преступлений // Виктимология. – 2014. – № 2(2). – С. 47-50.

215. Смагин П.Г. О понятии «Компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник ВИ МВД России. – 2008. – № 1. – С. 80-81.

216. Смирнова И.Г., Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Baikal Research Journal. 2015. №. 3 (6). – URL: http://brj-bguep.ru/ (дата обращения: 07.02.2025).

217. Смушкин А.Б. Отдельные аспекты использования искусственного интеллекта в криминалистической деятельности // В сборнике: Следственная деятельность. сборник научных трудов. – Минск, 2023. – С. 303-317.

218. Соколов А.Б., Щербина Р.П., Шаевич А.А. Криминалистически

значимая информация, хранящаяся в альтернативных потоках данных файловой системы NTFS // Криминалистика: вчера, сегодня, завтра. – 2022. – № 2 (22). – С. 159-169.

219. Сокольникова В.А. Информация и информационно-коммуникативные технологии (ИТ) в эпоху современной глобализации // Пробелы в российском законодательстве. – 2014. – № 6. – С. 286-291.

220. Соя-Серко Л.А. Программирование и творчество в деятельности следователя // Проблемы предварительного следствия в уголовном судопроизводстве. - М.: Изд-во Всесоюзного ин-та по изучению причин и разработке мер предупреждения преступности. – 1980. – С. 32-47.

221. Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. – 2014. – № 1(68). – С. 16-20.

222. Степанов-Егиянц В.Г. К вопросу о месте совершения компьютерных преступлений // Армия и общество. – 2014. – № 5(42). – С. 16-20.

223. Степаненко Д. А., Бахтеев Д. В., Евстратова Ю. А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. – 2020. – №. 2(14). – С. 206-214.

224. Сукманов А.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений // Вестник Калининградского Филиала Санкт-Петербургского университета МВД России. – Калининград, 2010. – № 4. – С. 104-107.

225. Телепнев П.Ф. Научный взгляд на определение понятия оперативно-розыскной информации // Вестник Санкт-Петербургского университета МВД России, 2016. – № 1(69). – С. 135-139.

226. Тулегенов В.В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. – 2014. – № 2(33). – С. 94-97.

227. Ульянов А.Д. Информационно-аналитическое обеспечение управленческой деятельности в органах внутренних дел // Вестник ВИ МВД

России. – 2007. – № 1. – С. 37-39.

228. Филимонов С.А. Некоторые проблемы борьбы с киберпреступностью как самых опасных транснациональных преступлений // APRIORI. Серия: Гуманитарные науки. – 2014. – № 1. – С. 25-33.

229. Хамидуллин Р.С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Электронное приложение к Российскому юридическому журналу. – 2024. – № 2. – С. 19-29.

230. Цимбал В.Н. Понятие, сущность и научное значение криминалистически значимой информации // Вестник КРУ МВД России. – 2010. – № 2. – С. 96-98.

231. Шаров В.И. Интернет как источник оперативно-разыскной и процессуальной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 3(35). – С. 111-114.

232. Швец С.В. Особенности следственной ситуации и применения тактических приемов на допросе с участием переводчика // Теория и практика общественного развития. – 2012. – № 4. – С. 387-391.

233. Швец С.В., Павлюков В.В. Преодоление средств компьютерной защиты как необходимый способ реализации оперативно-розыскного мероприятия «Получение компьютерной информации» // Общество: политика, экономика, право – 2018. – № 6. [Электронный ресурс]. – URL: https://doi.org/10.24158/pep.2018.6.15/ (дата обращения: 20.01.2025).

234. Швец С.В. Информационные особенности криминалистической деятельности в условиях перевода // Теория и практика общественного развития. – 2014. – № 5. – С. 235-237.

235. Швец С.В. Методические вопросы судебно-лингвистической экспертизы // Судебная экспертиза. – 2008. – № 1. – С. 91-96.

236. Щеголева Н.Л., Туяка А.К. К вопросу совершенствования современных габитоскопических регистрационно-поисковых систем // Вестник Санкт-Петербургского университета МВД России. – 2013. – № 3(59). – С. 223-231.

237. Шмидт А.А. К вопросу о классификации ОРМ «Наведение справок» // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2006. – № 6. – С. 67-69.

238. Шурухнов Н.Г. Современная преступность (истоки, направленность, техническая оснащенность, способы совершения, сокрытия): содержание рекомендаций по раскрытию и расследованию // Известия ТулГУ. Экономические и юридические науки. – 2013. – № 4-2. – С. 123-136.

239. Юсупкадиева С.Н. Этапы и формы взаимодействия следователя с другими службами ОВД при раскрытии и расследовании преступлений // Фундаментальные и прикладные исследования: проблемы и результаты. – 2014. – № 10. – С. 260-265.

240. Якупов Р.Х. Некоторые особенности понятия информационного обеспечения деятельности оперативных подразделений органов внутренних дел по раскрытию краж из квартир // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2010. – № 1(12). – С. 201-206.

Диссертации и авторефераты диссертаций:

241. Борисова Л.В. Транснациональные компьютерные преступления как объект криминалистического исследования: автореф. дис. … канд. юрид. наук: 12.00.09 / Борисова Лариса Владимировна. – К., 2007. – 22 с.

242. Вязовец Р.Н. Использование информационных технологий в оперативно-розыскной деятельности органов внутренних дел: автореф. дис. … канд. юрид. наук: 12.00.09 / Вязовец Роман Николаевич. – М., 2010. – 205 с.

243. Дерюгин Р.А. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия и использование его результатов при расследовании преступлений: дис. ... канд. юрид. наук: 12.00.12 / Дерюгин Роман Александрович. – Екатеринбург, 2018. – 226 с.

244. Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / Зиновьева Нина Сергеевна. – Краснодар, 2020. – 207 с.

245. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / Касаткин Андрей Валерьевич. – М., 1997. − 215 с.

246. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. – М, 2018. – 199 с.

247. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: дис. … канд. юрид. наук: 12.00.09 / Лыткин Николай Николаевич. – М., 2007. – 201 с.

248. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук: / Владимир Алексеевич Мещеряков – Воронеж, 2001. – 39 с.

249. Огородов Д.В. Правовые отношения в информационной сфере. дис. … канд. юрид. наук: 12.00.09 / Огородов Дмитрий Владимирович. – М., 2002. – 240 с.

250. Погосян Г.А. Проблемы получения и использования криминалистически значимой информации в качестве доказательств на предварительном следствии: Процессуальные и криминалистические аспекты: дис. … канд. юрид. наук: 12.00.09. – Краснодар, 2006. – 259 с.

251. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – М., 2016. − 232 с.

252. Родивилина В.А. Процессуальные особенности использования технических средств в стадии предварительного расследования дис. ... канд. юрид. наук / Родивилина Виктория Александровна. – Иркутск. 2016. – 218 с.

253. Свашенко Д.С. Планирование расследования налоговых преступлений дис. ... канд. юрид. наук / Сващенко Дмитрий Сергеевич. – Краснодар, 2016. – 238 с.

254. Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) дис. ... д-ра юрид. наук: 12.00.08 / Степанов-Егиянц

Владимир Георгиевич. – М., 2016. – 389 с.

255. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук: 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2010. – 206 с.

256. Суворова Л.А. Идеальные следы в криминалистике: дис. … канд. юрид. наук: 12.00.09 / Суворова Людмила Александровна. – Воронеж, 2005. – 245 с.

257. Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук: 5.1.4 / Харина Елена Алексеевна. – Красноярск – 2024. – 248 с.

258. Хорунжий С.Н. Следы в криминалистике и особенности их выявления и использования при расследовании групповых преступлений: дис. … канд. юрид. наук: 12.00.09 / Хорунжий Сергей Николаевич. – Воронеж, 2001. – 224 с.

259. Швец С.В. Криминалистическая тактика следственных и судебных действий в условиях использования перевода: автореф. д-ра юрид. наук / Швец Сергей Владимирович. – Краснодар, 2014. – 59 с.

260. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук: 12.00.12 / Шевченко Елизавета Сергеевна. – Москва, 2016. – 249 с.

Электронные ресурсы:

261. Анализ системы вывода денежных средств, похищенных у граждан [Электронный ресурс]. Сайт sberbank.ru URL: https://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv?tab=analiz_problemy (дата обращения: 18.02.2025).

262. Большой и заботливый брат [Электронный ресурс]. – URL: https://tjournal.ru/p/google-for-surveillance-reform (дата обращения: 22.02.2025).

263. Большой обзор свежих эксплойт-пакетов. [Электронный ресурс]. – URL: https://xakep.ru/2015/04/09/195-exploit-packs/ (дата обращения: 22.02.2025).

264. Введение: почему мы решили анализировать Java. [Электронный ресурс]. – URL: https://securelist.ru/analysis/obzor/20794/otchet-laboratorii-

kasperskogo-java-pod-udarom-evolyuciya-eksplojtov-v-2012-2013-gg/ (дата обращения: 22.02.2025).

265. «Военная разведка» [Электронный ресурс] // Онлайн энциклопедия «Кругосвет». – URL: http://www.krugosvet.ru/enc/nauka_i_tehnika/ (дата обращения: 11.02.2025).

266. Госдума приняла антитеррористический пакет Ирины Яровой [Электронный ресурс]. – URL: http://pravo.ru/news/view/130575 (дата обращения: 26.02.2025).

267. Дуров: блокировка Telegram не поможет в борьбе с терроризмом – [Электронный ресурс]. – URL: http://www.ntv.ru/novosti/1826858/ (дата обращения: 27.01.2025).

268. Единая система информационно-аналитического обеспечения деятельности МВД РФ Ход проекта [Электронный ресурс]. – URL: http://www.tadviser.ru/index.php/Проект:Единая_система_информационно-аналитического_обеспечения_деятельности__МВД_РФ_(ИСОД_МВД) (дата обращения: 04.02.2025).

269. Законодательство Республики Казахстан – URL: https://www.zakon.kz/221107-sravnitelnyjj-analiz-mezhdunarodnykh.html (дата обращения: 02.02.2025).

270. За кулисами мошенничества [Электронный ресурс]. Сайт sberbank.ru URL: https://www.sberbank.ru/ru/person/kibrary/investigations/berdyansk-glava-5 (дата обращения: 07.03.2025).

271. Запросы личной информации в Google [Электронный ресурс] // Отчет о доступности сервисов и данных Google. URL: https://transparencyreport.google.com/user-data/overview?hl=ru (дата обращения: 13.02.2025).

272. Зарегистрировать домен [Электронный ресурс]. – URL: https://www.reg.ru/domain/new (дата обращения: 30.01.2025).

273. Информационный ресурс «cnews.ru» МВД потратит 70 млн руб., чтобы уничтожить приватность в Рунете [Электронный ресурс]. – URL:

http://www.cnews.ru/news/top/mvd_potratit_70_mln_rub.chtoby_unichtozhit (дата обращения: 22.01.2025).

274. Информационный ресурс «cnews.ru» МВД строит Единую информационно-аналитическую систему за 1,5 млрд руб. [Электронный ресурс]. – URL:http://www.cnews.ru/news/top/mvd_stroit_edinuyu_informatsionnoanaliticheskuyu (дата обращения: 22.01.2025).

275. К Яровой нет ключа [Электронный ресурс]. – URL: http://www.vedomosti.ru/newspaper/articles/2017/02/16/678086-yarovoi-klyucha (дата обращения: 07.02.2025).

276. Лоскутов И.Ю. Сравнительный анализ международных норм законодательного регулирования Интернета в различных странах (2008 год) [Электронный ресурс]. – URL: http://www.zakon.kz/221107-sravnitelnyjj-analiz-mezhdunarodnykh.html (дата обращения: 28.01.2025).

277. Логирование информации [Электронный ресурс]. – URL: http://hostinfo.ru/articles/security/rubric157/1062/ (дата обращения: 15.02.2025).

278. Мария Нефедова Публикация VAULT 7 // Журнал «Хакер». № 218 март 2017.

279. МВД РФ создает поисковую систему, которая позволит по фотороботу быстро найти человека [Электронный ресурс]. – URL: http://www.newsru.com/russia/24sep2008/proekt.html (дата обращения: 15.01.2025).

280. Медведев оценил в полтриллиона долларов ущерб от киберпреступлений в мире. [Электронный ресурс] Интерфакс. – URL: http://www.interfax.ru/business/511660 (дата обращения: 22.02.2025).

281. Моделирование угроз на основе сценариев или как Cyber Kill Chain и ATT&CK помогают анализировать угрозы ИБ URL: https://safe-surf.ru/specialists/article/5247/626649/ (дата обращения:13.02.2025).

282. Оперативное получение компьютерной информации // Жизнь в законе, портал для ликвидации юридической безграмотности [Электронный ресурс]. – URL: http://lifeinlaw.ru/bez-rubriki/orm.php (дата обращения: 22.02.2025).

283. Парсинг: Что? Зачем? Как? [Электронный ресурс]. – URL:

http://parsing.valemak.com/ (дата обращения: 22.01.2025).

284. Пользователи Gmail могут не рассчитывать на тайну переписки [Электронный ресурс]. – URL: http://www.cnews.ru/news/top/google_polzovateli_gmail_mogut_ne (дата обращения: 18.02.2025).

285. Перехват данных: кто, где и как [Электронный ресурс]. – URL: http://www.nestor.minsk.by/sr/2007/01/sr70102.html (дата обращения: 24.01.2025).

286. Путин отказался подписать Конвенцию о киберпреступниках [Электронный ресурс]. – URL: http://safe.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu (дата обращения: 03.02.2025).

287. Полицейские Хабаровского края рассказали о работе автоматизированной информационно-поисковой системы «Портрет-Поиск» от 13.08.2015 [Электронный ресурс]. – URL: https://27.mvd.ru/news/item/6328745/ (дата обращения: 29.01.2025).

288. Русскоязычный информационный сайт о криптовалюте Bitcoin [Электронный ресурс]. – URL: https://bits.media/silk-road/ (дата обращения: 20.02.2025).

289. Теракты в лондонском метро 7 июля 2005 года. Справка [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/defense_safety/20090707/176530177.html (дата обращения: 24.02.2025).

290. Страшный и ужасный COPM2: немного практики [Электронный ресурс]. URL: https://habr.com/ru/post/65924/ (дата обращения: 13.02.2025).

291. Портал правовой статистики [Электронный ресурс] // Генеральная прокуратура Российской Федерации. – URL: http://crimestat.ru/analytics (дата обращения: 01.02.2025).

292. МВД назвало число преступлений, совершенных с использованием IT-технологий [Электронный ресурс] РИА Новости // – URL: https://ria.ru/20250218/kompaniya-1999981895.html (дата обращения: 18.02.2025).

293. С 1 марта Google официально следит за каждым. [Электронный

ресурс]. – URL: http://techno.bigmir.net/technology/1516551-S-1-marta-Google-oficial-no-sledit-za-kazhdym- (дата обращения: 20.02.2025).

294. Форум сотрудников ОВД [Электронный ресурс]. – URL: https://www.police-russia.ru/showthread.php?p=3553535 (дата обращения: 12.01.2025).

295. Шифр и меч, ФСБ собирается взять интернет-трафик на контроль [Электронный ресурс] // «Коммерсант». – URL: http://kommersant.ru/doc/3094848 (дата обращения: 22.01.2025).

296. Чем занимается «белый хакер», как им стать и сколько можно заработать [Электронный ресурс]. – URL: https://vc.ru/story/86714-chem-zanimaetsya-belyy-haker-kak-im-stat-i-skolko-mozhno-zarabotat?from=digest&date=081019 (дата обращения: 12.01.2025).

297. Что такое эксплойты и почему их все так боятся? [Электронный ресурс]. – URL: https://blog.kaspersky.ru/exploits-problem-explanation/8459/ (дата обращения: 09.02.2025).

298. Эксплойт-пак для новичков. [Электронный ресурс]. – URL: http://www.truehackers.ru/articles/vulnerabilities/4394-jeksplojtpak-dlja-novichkov (дата обращения: 28.01.2025).

299. Ястребов Д.А. Понятие, объективные признаки, объект и предмет неправомерного доступа к компьютерной информации [Электронный ресурс] // Информационные материалы для студентов. – URL: https://superinf.ru/view_helpstud.php?id=478 (дата обращения: 04.02.2025).

300. Яровая объяснила, для чего нужен новый пакет законов [Электронный ресурс]. – URL: http://www.vestifinance.ru/articles/72602 (дата обращения: 25.01.2025).

301. Яндекс-Диктовка [Электронный ресурс]. – URL: http://speech-soft.ru/prog/yandeksdiktovka (дата обращения: 29.01.2025).

302. AI can detect abusive messages 21 times faster than humans - Forensic Capability Network. [Электронный ресурс]. – URL: https://www.fcn.police.uk/news/2024-07/ai-can-detect-abusive-messages-21-times-

faster-humans (дата обращения: 13.02.2025).

303. Social Searcher Free Social Media Search Engine [Электронный ресурс]. – URL: https://www.social-searcher.com/ (дата обращения: 19.01.2025).

304. Google сотрудничает с силовиками [Электронный ресурс]. – URL: https://wek.ru/google-sotrudnichaet-s-silovikami (дата обращения: 12.02.2025).

305. FindFace: российская программа распознавания лиц завоевывает мир [Электронный ресурс]. – URL: http://www.vesti.ru/doc.html?id=2723304 (дата обращения: 09.01.2025).

306. What is AWStats [Электронный ресурс]. – URL: http://www.awstats.org (дата обращения: 03.02.2025).

307. About What is Wikileaks? [Электронный ресурс]. – URL: https://www.wikileaks.org/About.html (дата обращения: 26.01.2025).

308. Bills S.436 and H.R. 1076, Their to protect the children! No, it’s not and we know it fucktard [Электронный ресурс]. – URL: https://krypt3ia.wordpress.com/2009/02/21/bills-s436-and-hr-1076-their-to-protect-the-children-no-its-not-and-we-know-it-fucktard/ (дата обращения: 25.01.2025).

309. U.S. appeals court upholds gag orders on FBI data surveillance [Электронный ресурс]. URL: http://www.reuters.com/article/us-usa-surveillance-idUSKBN1A21XJ (дата обращения: 25.01.2025).

310. Mass surveillance [Электронный ресурс]. – URL: https://www.revolvy.com/topic/Mass%20surveillance&item_type=topic (дата обращения: 06.02.2025).

311. Telecommunications data retention [Электронный ресурс]. – URL: https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Telecommunications_data_retention.html (дата обращения: 18.02.2025).

312. John Lettice Gatso 2: rollout of UK's '24x7 vehicle movement database' begins [Электронный ресурс]. – URL: https://www.theregister.co.uk/2005/11/15/vehicle_movement_database (дата обращения: 19.02.2025).

Приложение 1

Опросный лист

РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ 100 СОТРУДНИКОВ ОВД ЛНР, ДНР, г. Севастополь

№ п/п	Вопрос анкеты	Варианты ответов	Результаты,%
1	По вашему мнению, позволяет ли действующее законодательство РФ получить быстрый доступ к компьютерной информации в процессе расследования преступлений?	1. Да. 2. Нет. 3. Затрудняюсь ответить.	56% 44% -
2	По вашему мнению, какие оперативно-розыскные мероприятия Вы провели бы с целью поиска компьютерной информации в процессе расследования преступлений:	1. Опрос. 2. Наведение справок. 3. Сбор образцов для сравнительного исследования. 4. Проверочная закупка. 5. Исследование предметов и документов. 6. Наблюдение. 7. Отождествление личности. 8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств. 9. Контроль почтовых отправлений, телеграфных и иных сообщений. 10. Прослушивание телефонных переговоров. 11. Снятие информации с технических каналов связи. 12. Оперативное внедрение. 13. Контролируемая поставка. 14. Оперативный эксперимент. 15. Получение компьютерной информации.	- - 92 % - - - - - 17% 87% 70% - - -
3	По вашему мнению, какое оперативно-розыскное мероприятие, в том числе предложенное автором «Компьютерная разведка», вы бы первоначально использовали при получении компьютерной информации:	1. Снятие информации с технических каналов связи. 2. Получение компьютерной информации. 3. Компьютерная разведка. 4. Затрудняюсь ответить.	14% 30% 54% 2%
4	По вашему мнению, должны ли ОРМ «Получение компьютерной информации» и «Снятие информации с технических каналов связи» осуществляться совместно:	1. Да, должны осуществляться совместно. 2. Нет, возможно осуществлять раздельно. 3. Затрудняюсь ответить.	83% 5% 12%
5	По вашему мнению, ускорится ли процесс получения информации при объединении компьютерной информации из сети Интернет с банками данных ОВД:	1. Да. 2. Нет. 3. Затрудняюсь ответить.	81% 19%
6	По вашему мнению, целесообразно ли получать логины и пароли от баз данных сайтов и аккаунтов пользователей с целью получения компьютерной информации:	1. Да. 2. Нет. 3. Затрудняюсь ответить.	94% 6% -
7	Необходимо ли в неотложных ситуациях прибегать к методам преодоления компьютерной защиты, позволяющим оперативно получить информацию без предварительной судебной санкции (но с обязательным последующим судебным контролем), если есть основания полагать, что такая информация	1. Да. 2. Нет. 3. Затрудняюсь ответить.	92% 2% 6%

	имеет оперативное значение:		
8	По вашему мнению, облегчится ли взаимодействие между сотрудниками ОВД, если запросы на предоставление информации будут передаваться при помощи компьютерных систем и сетей?	1. Да. 2. Нет. 3. Затрудняюсь ответить	83% 13% 4%
9	Привлекали ли Вы специалиста в области информационных технологий при расследовании преступлений, совершаемых в сфере компьютерной информации	Привлекали Не привлекали	2% 98%
10	По вашему мнению, будут ли для Вас иметь оперативный интерес граждане, которые обращались к ресурсам с запрещенными материалами, размещенными в сети Интернет:	1. Да. 2. Нет. 3. Затрудняюсь ответить.	78% 12% 10%
11	По вашему мнению, сколько времени должны хранить компьютерную информацию провайдеры о деятельности пользователей в компьютерной сети:	1. 1 день. 2. 1 месяц. 3. 3-6 месяцев. 4. 6 – 12 месяцев. 5. 1 год и более 6. Хранить должны после запроса от сотрудника ОВД. 7. Затрудняюсь ответить.	3% 30% 55% 10% 2%
12	По вашему мнению, считаете ли вы необходимым сбор и анализ компьютерной информации в сети интернет и объединение ее с банками данным МВД о гражданах, которые ранее привлекались за административные и уголовные правонарушения:	1. Да. 2. Нет. 3. Затрудняюсь ответить.	79% 5% 16%
13	Получали ли вы добровольное согласие на получение доступа к компьютерной информации от подозреваемого?	1. Да. 2. Нет. 3. Затрудняюсь ответить.	97% 3% -

Приложение 2

РЕЗУЛЬТАТЫ АНАЛИЗА 50 СУДЕБНЫХ РЕШЕНИЙ, ГДЕ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ИСПОЛЬЗОВАЛАСЬ КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ

В ходе анализа 60 судебных решений открытой судебной практики Российской Федерации, в рамках которых проводились ОРМ, следственные и различные действия, направленные на получение компьютерной информации, было установлено, что:

- ОРМ проводилось на основании постановления суда в 5 делах, в остальных случаях это было добровольное согласие или мероприятие проводилось без санкций;

- ОРМ, в основном такое как «Получение компьютерной информации», осуществлялось путем просмотра социальной сети vk.com – в 37 судебных решениях, социальной сети ok.ru – 1 дело, доски объявлений – 4 дела, сайта www.nvspc.com – 2 дела, сайт - https://probive.one. Путем осмотра мобильного телефона в 10 делах, где в 7 делах указано о том, что информация была получена в мессенджере «Telegram», в 2-х делах с мессенджера «WhatsApp», в папке «Галерея», находящейся в мобильном телефоне – 3 дела, в папке «Диктофон» – 1 дело.

Следует отметить, что в ходе проведенного анализа судебных решений установлено, что с целью фиксации последних полученная информация в 20 делах фиксировалась при помощи скриншотов. Также в 6 решениях было указано, что с целью установления личности и дополнительной информации о пользователе был сделан запрос владельцу интернет-ресурса.

№	Судебные решения	Статьи	Способы получения компьютерной информации	Способы фиксации компьютерной информации
1	Постановление № 5-236/2019 от 12.02.2019 г.	ч.1 ст. 20.3 КоАП	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - скриншоты Интернет-страниц; - объяснение подозреваемого, не отрицавшего факт совершения административного правонарушения.
2	Постановление № 5-4/2019 от 15.01.2019 г.	ст. 20.29 КоАП	Осмотр Интернет страницы	- протокол опроса подозреваемого; - протокол ОРМ «ПКИ»;

			(vk.com)	- фототаблица.
3	Приговор № 1-16/2019 1-360/2018 от 09.01.2019 г.	ч.3 ст. 30 п. «г» ч.4 ст.228.1 УК РФ	Осмотр Интернет страницы (www.nvspc.com), на основании постановления суда	- акт о результатах ОРМ «ПКИ»; - предложено предоставить информацию с сайта, на что подозреваемый дал свое согласие; - постановление о рассекречивании сведений, составляющих государственную тайну и их носителей;
4	Постановление № 5-2480/2018 от 23.11.2018 г.	ст.20.29 КоАП	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - объяснение подозреваемого;
5	Постановление № 5-3613/2018 от 2.11.2018 г.	ч.1 ст. 20.3 КоАП РФ	Осмотр Интернет страницы (ok.ru)	- акт о проведении ОРМ «ПКИ»; - скриншоты;
6	Приговор № 1-275/2018 от 18.10.2018 г.	ч. 3 ст. 30 п. Г ч. 4 ст. 228.1, ч. 2 ст. 228 УК РФ	Осмотр мобильного телефона (Telegram)	- протокол ОРМ «ПКИ»;
7	Приговор № 1-86/2018 от 24.09.2018 г.	ч.3 ст.30 п. «г» ч.4 ст.228.1 УК РФ	Осмотр мобильного телефона (Telegram), на основании постановления суда	- протокол личного досмотра; - постановление о предоставлении результатов оперативно-розыскной деятельности следователю или в суд, в соответствии с которым предоставлен акт проведения ОРМ «ПКИ»; - протокол осмотра предметов; - акт проведения ОРМ «ПКИ», где установлено наличие переписки с «yinyang» на 23 листах с фото с изображением расположения закладки; - постановление суда в ПАО «Мегафон» о получении информации о соединениях абонентского номера;
8	Приговор № 1-60/2018 от 26.07.2018 г.	ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1; ч. 3 ст. 30, ч. 5 ст. 228.1; ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1; п. «г» ч. 4 ст. 228.1; п. «а» ч. 3 ст. 228.1; п. «г» ч. 4 ст. 228.1 УК РФ	Осмотр мобильного телефона	- результаты ОРМ «ПКИ»; - компакт-диск с результатами ОРМ «ПКИ».
9	Решение № 12-40/2018 от 25.05.2018 г.	ч. 4 ст. 5.26 КоАП РФ	Путем запроса в поисковой системе и осмотром найденной интернет страницы объявлений	- акт о проведении ОРМ «ПКИ»; - скриншоты Интернет-страниц; - объяснение подозреваемого;
10	Постановление № 7-1270/2017 от 25.10.2017	ст.20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - письменное объяснение;
11	Постановление № 5-3878/2017 5-3978/2017 от 6 ноября 2017	ст.20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт ОРМ «ПКИ»; - компакт-диск; - заключение специалиста в области лингвистики.
12	Постановление № 5-35/2018 от 17.05.2018 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншот экрана монитора страницы пользователя сайта; - протокол опроса подозреваемого;

				- компакт-диск, содержащий записи с результатом осмотра страницы пользователя социальной сети; - выписка из федерального списка экстремистских материалов.
13	Приговор № 1-458/2017 1-63/2018 от 2.02.2018 г.	ч. 3 ст. 30 п. «г» ч. 4 ст. 228.1 УК РФ	Осмотр мобильного телефона (www.nvspc.org)	- акт по результатам проведения ОРМ «ПКИ»; - фото в галерее телефона; - скриншоты экрана монитора страницы пользователя сайта.
14	Постановление № 5-4085/2017 от 7.12.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт результатов ОРМ «ПКИ»;
15	Приговор № 1-244/2017 от 17.11.2017 г.	ч.3 ст.30 - п.«г» ч.4 ст.228.1 и ч.1 ст.228 УК РФ	Осмотр мобильного телефона и вход путем получения пароля	- справка по результатам проведения ОРМ «ПКИ»; - скриншоты экрана телефона.
16	Постановление № 5-383/2017 от 13.11.2017 г.	ст.20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- рапорт об обнаружении признаков правонарушения; - акт о проведении ОРМ «ПКИ» - скриншоты экрана монитора страницы пользователя сайта; - объяснение пользователя с признанием вины; - выписки из федеральных списков экстремистских материалов;
17	Приговор № 1-322/2017 от 9.11.2017 г.	ч.3 ст.30 п. «г» ч.4 ст.228.1 УК РФ	Осмотр мобильного телефона (www.nvspc.com), где поступило указание и вынесено постановление начальника о проведении ОРМ «ПКИ» из мобильного телефона	- справка по результатам проведения ОРМ «ПКИ»; - заключение эксперта об использовании телефона для посещения сайта «http:www.nvspc.com»; скриншоты с экрана мобильного телефона; - информация об использовании сервисов «Visa QIWI кошелек»; Получено добровольное согласие от подозреваемого на осмотр мобильного телефона «Huawei». В присутствии понятых телефон был исследован. В телефоне были найдены описания тайниковых закладок в Интернете. Мобильный телефон был подключен к компьютеру «Packard Bell».
18	Постановление № 7-1270/2017 от 25.10.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - распечатка скриншотов страницы в социальной сети;
19	Приговор № 1-254/2017 от 16.10.2017 г.	ч.3 ст.30-п. «г» ч.4 ст.228.1 УК РФ	Осмотр Интернет страницы (Интернет магазин, vk.com) Осмотр программ VIPole, Telegram, Jabber, на основании постановления суда	- протокол ОРМ «ПКИ»; - протоколы исследования планшета, системного блока;
20	Постановление № 5-1163/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; - справка об установлении пользователя социальной сети «ВКонтакте».

21	Постановление № 5-1167/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; ответ на запрос; - справка об установлении пользователя социальной сети «ВКонтакте».
22	Постановление № 5-1164/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	осмотра Интернет страниц (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; ответ на запрос; - справка об установлении пользователя социальной сети «ВКонтакте».
23	Постановление № 5-1166/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; ответ на запрос; - справка об установлении пользователя социальной сети «ВКонтакте».
24	Постановление № 5-1168/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; ответ на запрос; - справка об установлении пользователя социальной сети «ВКонтакте».
25	Постановление № 5-1165/2017 от 13.10.2017 г.	ст.20.29. КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - запрос заместителю генерального директора по безопасности ООО «В Контакте»; ответ на запрос; - справка об установлении пользователя социальной сети «ВКонтакте».
26	Постановление № 5-1341/2017 от 22.08.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - фотографии; - в ходе опроса подозреваемая пояснила, что указанная страница в социальной сети «В Контакте» принадлежит ей.
27	Приговор № 1-164/2017 от 18.08.2017 г.	ч.3 ст.30 п. «г» ч.4 ст.228.1 УК РФ	Осмотр мобильного телефон (WhatsApp), на основании постановления суда	- справка по результатам проведения ОРМ «ПКИ»; - компакт-диск с материалами ОРМ «ПКИ».
28	Постановление № 5-637/2017 от 16.06.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - справка об установлении пользователя социальной сети «ВКонтакте».
29	Приговор № 1-130/2017 от 17.05.2017 г.	ч.3 ст.30 п. «г» ч.4 ст.228.1 УК РФ	Осмотр мобильного телефона и планшета (Telegram) на основании постановления суда о проведении ОРМ «ПКИ»	- справка по результатам проведения ОРМ «ПКИ»; - в папке «Диктофон» мобильного телефона, были обнаружены тринадцать аудио файлов с записью адресов, где ранее были заложены наркотические средства; - аудио файлы скопированы на оптический диск.
30	Постановление № 5-537/2017 от 15.05.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ».

31	Решение № 12-17/2017 от 18.04.2017 г.	ч.4 ст.5.26 КоАП РФ	Осмотр Интернет страницы (доска объявлений, сайт братства ХВЕП)	- акт о проведении ОРМ «ПКИ»; - скриншоты веб-страниц; - объяснение подозреваемого.
32	Постановление № 5-140/2017 от 6.03.2017 г.	ст.20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - фотоматериалы; - в судебном заседании подозреваемый вину в совершении административного правонарушения признал и пояснил, что указанная страница в социальной сети «В Контакте» принадлежит ему.
33	Постановление № 5-671/2016 от 20.12.2016 г.	ч. 1 ст. 20.3 КоАП РФ	Осмотр Интернет страницы (доска объявлений)	- акт о проведении ОРМ «ПКИ»; - протокол опроса подозреваемого с признанием вины.
34	Приговор № 1-31/2019 от 25.02.2019 г.	п.«г» ч.4 ст.228.1 УК РФ	Осмотр мобильного телефона (WhatsApp)	- результаты ОРМ «ПКИ»; - протокол соединений абонентского номера; - диск с видеозаписью.
35	Постановление № 5-143/2018 от 17.09.2018 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншоты экранов; - справка об установлении пользователя социальной сети «Вконтакте»; - компакт-диск CD-R.
36	Приговор № 1-218/2018 от 18.05.2018 г.	ст.138.1 УК РФ	путем исследования информационных поисковых сетей (доска объявлений https://youla.io)	- акт о проведении ОРМ «ПКИ»; - компакт диск.
37	Приговор № 1-415/2017 1-8/2018 от 14.02.2018 г.	ч.3 ст. 30 п. «г» ч.4 ст. 228.1 УК РФ	осмотра мобильного телефона **(**Telegram**),** где на проведение ОРМ «ПКИ» получено постановление суда	- Постановление о предоставлении результатов оперативно-розыскной деятельности.
38	Постановление № 7-1028/2017 от 6.10.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - протокол опроса, согласно которого подозреваемый пояснил, что он является пользователем социальной сети «ВКонтакте» под условным именем «Г...» (https://vk.com /….).
39	Постановление № 7-1030/2017 от 21.09.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - протокол опроса, согласно которого подозреваемый в присутствии законного представителя несовершеннолетнего пояснил, что он является пользователем социальной сети «ВКонтакте» под условным именем «Б...» (https://vk.com /….).
40	Постановление № 7-932/2017 от 17.08.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - письменное объяснение подозреваемого, где последний владеет профилем пользователя https:// vk.com/…
41	Постановление № 7-1027/2017 от 21.09.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - протокол опроса, согласно которого подозреваемая пояснила, что она является пользователем социальной сети «ВКонтакте» под условным именем «С..».

42	Постановление № 7-1025/2017 от 21.09.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - протокол опроса, согласно которого подозреваемый пояснил, что он является пользователем социальной сети «ВКонтакте» под условным именем «У…» (https://vk.com/....).
43	Постановление № 7-973/2017 от 25.08.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - объяснение, согласно которому аудиозапись находилась на интернет-странице социальной сети «ВКонтакте» и принадлежала ему.
44	Постановление № 5-89/2017 от 18.01.2017 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- справка о проведении ОРМ «ПКИ»; - рапорт об обнаружении признаков административного правонарушения; - протоколы опроса; - справка об установлении пользователя социальной сети «ВКонтакте».
45	Постановление № 5-2442/2016 от 25.11.2016 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - справка об установлении пользователя социальной сети «ВКонтакте».
46	Постановление № 5-1007/2018 от 20.11.2018 г.	ч. 1 ст. 20.3 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншоты экрана монитора страницы пользователя сайта;
47	Постановление № 5-319/2016 от 18.11.2016 г.	ст.20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншоты экрана монитора страницы пользователя сайта.
48	Постановление № 5-135/2018 от 18 мая 2018 г.	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншоты экрана монитора страницы пользователя сайта; - объяснение подозреваемого, в котором он пояснил, что в социальной сети «ВКонтакте» он зарегистрирован под именем «П…».
49	Постановление № 5-114/2018 от 11 июля 2018 г.	ст. 20.3 КоАП РФ	Осмотр Интернет страницы (vk.com)	- протокол ОРМ «ПКИ»; - скриншоты экрана монитора страницы пользователя сайта; - справка об установлении пользователя социальной сети «ВКонтакте».
50	Постановление № 5-1173/2017 от 16.10.2017	ст. 20.29 КоАП РФ	Осмотр Интернет страницы (vk.com)	- акт о проведении ОРМ «ПКИ»; - скриншот страницы «ВКонтакте».
51	Приговор № 1-33/2024 от 12 июля 2024 г. по делу № 1-33/2024	ч. 1 ст. 30, п. «в» ч. 2 ст. 226.1 УК РФ	мессенджер «WeChat»	- справка по результатам ОРМ « Получение компьютерной информации »
52	Приговор № 1-39/2024 1-493/2023 от 2 мая 2024 г. по делу № 1-39/2024	ч.2 ст. 282.1 УК РФ, ч.2 ст.213 УК РФ	Осмотр Интернет страницы (vk.com)	- протокол получения компьютерной информации
53	Приговор № 1-70/2024 1-730/2023 от 21 февраля 2024 г. по делу № 1-70/2024	ч. 4 ст. 228.1 УК РФ	приложения «WhatsApp»	- протокол получения компьютерной информации
54	Постановление № 5-78/2024 от 21 февраля 2024 г. по делу № 5-78/2024	ч.1 ст.20.3 КоАП РФ	мессенджер «Telegram»	протоколом «Получение компьютерной информации »
55	Постановление № 5-77/2024 от 21 февраля	ч.1 ст.20.3 КобАП	мессенджер «Telegram»	- справка по результатам проведения оперативно-розыскного мероприятия

	2024 г. по делу № 5-77/2024			«Получение компьютерной информации»
56	Приговор № 1-1219/2022 1-25/2024 1-276/2023 от 7 февраля 2024 г. по делу № 1-1219/2022	п. «а, г» ч. 4 ст. 228.1, ч. 3 ст. 30, п. «а,г» ч.4 ст. 228.1, ч. 3 ст. 30, ч. 5 ст. 228.1 УК РФ	интернет-приложения «Xabber»	справка по результатам оперативно-розыскного мероприятия «Получение компьютерной информации»
57	Приговор № 1-319/2024 от 5 июня 2024 г. по делу № 1-319/2024	ч.3 ст.272, ч.3 ст. 183 УК РФ	мессенджер «Telegram» сайт https://probive.one	ОРМ «сбор образцов для сравнительного исследования (осмотр сотового мобильного устройства) Скриншоты с информацией о сайте https://probive.one, полученные в ходе ОРМ «Получение компьютерной информации»
58	Постановление № 5-10/2024 от 30 января 2024 г. по делу № 5-10/2024	ч. 1 ст. 20.3 КоАП РФ	Осмотр https://vk.com/	протокол получения компьютерной информации
59	Решение № 12-27/2024 от 17 июня 2024 г. по делу № 12-27/2024	ч. 4 ст. 5.26 КоАП РФ	мессенджер «Telegram»	протокол получения компьютерной информации
60	Постановление № 5-160/2024 от 11 июня 2024 г. по делу № 5-160/2024	ч. 1 ст. 20.3 КоАП РФ	Скриншоты изобрашений страницы пользователя социальной сети «vk.com»	протокол ОРМ «Получение компьютерной информации»