**Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»**

На правах рукописи

**Белова Ксения Сергеевна**

# ТАКТИКО-ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

5.1.4. Уголовно-правовые науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Кисленко Сергей Леонидович

Москва — 2026

# ОГЛАВЛЕНИЕ

**ВВЕДЕНИЕ ..... 3**
**ГЛАВА I. ЗАДАЧИ И НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ..... 16**
§ 1. Сеть «Интернет» как объект изучения криминалистической науки 16
§ 2. Основные направления поисково-познавательной деятельности следователя по использованию сети «Интернет»..... 52
**Глава II. АЛГОРИТМЫ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» В ЦЕЛЯХ ПОЛУЧЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ..... 79**
§ 1. Использование ресурсов сети «Интернет» в установлении информации о событии преступления и совершившем его лице..... 79
§ 2. Изучение личности совершившего преступление, его розыск и изобличение с использованием ресурсов сети «Интернет»..... 102
**ГЛАВА III. ТАКТИКО-ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ..... 148**
§ 1. Особенности использования сети «Интернет» при производстве невербальных следственных действий ..... 148
§ 2. Особенности использования сети «Интернет» при производстве вербальных следственных действий ..... 185
**ЗАКЛЮЧЕНИЕ ..... 210**
**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ..... 220**
**ПРИЛОЖЕНИЯ ..... 257**
*Приложение 1.* Результаты анкетирования работников подразделений органов следствия и дознания по вопросам использования информационно-телекоммуникационной сети «Интернет» при расследовании преступлений ……...257
*Приложение 2.* Перечень основных криминалистически значимых сведений из цифрового профиля гражданина России ..... 261

# ВВЕДЕНИЕ

**Актуальность темы исследования.** В XXI в. информационно-телекоммуникационная сеть «Интернет» превратилась в одну из наиболее востребованных технологий, обеспечивающую возможность работы с огромными массивами информации. Данные статистики свидетельствуют: в 2025 г. 5,56 млрд человек регулярно пользовались Интернетом (67,9 % живущих на Земле людей)[1]. Аудитория российского сегмента пользователей Сети в 2025 г. составила свыше 130 млн человек, что близко к численности населения страны.

Возможности сети «Интернет» позволяют законопослушным гражданам совершать множество действий онлайн: получать образование, работать удаленно, оплачивать товары и услуги и т.д. Однако, кроме позитивных перемен, цифровизация социума влечет за собой ряд негативных явлений, связанных с ростом противоправной активности, включая совершение преступлений с использованием ресурсов сети «Интернет». Происходят не только количественные, но и качественные изменения преступности. Сегодня интернет-технологии интегрируются в механизм самых разных преступлений, помимо тех, ответственность за которые предусмотрена главой 28 УК РФ «Преступления в сфере компьютерной информации». Настоящим вызовом современному обществу стал кратный рост едва ли не всех видов мошенничества из-за масштабов использования преступниками информационно-телекоммуникационных сетей и информационно-коммуникационных технологий[2].

Активное взаимодействие пользователей с сетью «Интернет» меняет следовую картину преступлений — сведения о человеке и его деятельности фиксируются в кодированном виде. Работа с такого рода следами вызывает

---

[1] Статистика пользователей интернета в мире и в России [Электронный ресурс] // URL: https://up-advert.ru/blog/digital-2025/ (дата обращения: 03.01.2026).

[2] См.: Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»; распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // СПС «Гарант».

затруднения у сотрудников правоохранительных органов, что негативно сказывается на результативности процесса раскрытия, расследования, пресечения и предупреждения преступлений, связанных с использованием информационно-коммуникационных технологий. По данным МВД России, уровень раскрываемости таких преступлений невысок: около 23 % — в 2024 г. и 29 % — в 2025 г.[3] Проблемы отчасти усугубляются из-за отсутствия унифицированных криминалистических рекомендаций по работе со следами в информационно-телекоммуникационной сети «Интернет».

Ранее разработанные методики расследования отдельных видов преступлений (прежде всего в сфере компьютерной информации) в современных условиях ввиду применения преступниками новых технологий теряют свою актуальность. Идентификация физического лица по следам-отображениям в физическом пространстве отличается от его идентификации как пользователя по следам в сети «Интернет». Правильное понимание специфики данного процесса крайне важно и для обеспечения законодательной регламентации порядка использования информационно-телекоммуникационных сетей, и для пресечения криминальной активности. Деятельность правоохранительных органов модифицируется: правоприменители все чаще обращаются к сети «Интернет» как источнику криминалистически значимой информации и технологическому ресурсу, обеспечивающему эффективность производства следственных действий.

Изложенное свидетельствует о необходимости уточнения с позиций криминалистики места цифровых технологий в механизме преступлений, уяснения криминалистически значимых аспектов процессов возникновения и отражения информации в информационно-телекоммуникационной сети «Интернет», а также специфики выявления, фиксации, изъятия и использования данных из интернет-ресурсов для получения сведений о преступной деятельности и ее участниках. Востребованность рекомендаций, направленных на повышение эффективности деятельности по использованию сети «Интернет» в целях решения задач

[3] URL: https://mvdmedia.ru/news/official/informatsiya-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-yanvar-noyabr-2025-goda/ (дата обращения: 10.05.2026).

предварительного расследования, обусловливает актуальность темы диссертации и свидетельствует о ее высоком исследовательском потенциале.

**Степень разработанности темы**. Организации расследования преступлений посвящен целый ряд трудов видных ученых: Р.С. Белкина, Т. С. Волчецкой, А. Ф. Волынского, В. Д. Зеленского, Е. П. Ищенко, Н. В. Кручининой, В. П. Лаврова, И. П. Можаевой, И. В. Тишутиной и др. Однако сеть «Интернет», использование ее возможностей не рассматривались ими в качестве самостоятельного объекта криминалистического исследования.

Тактика проведения следственных действий предметно анализировалась О. Я. Баевым, М. О. Баевым, Л. В. Бертовским, А. Н. Васильевым, Ю. П. Гармаевым, Л. Я. Драпкиным, А. В. Дуловым, И. М. Комаровым, В. И. Комиссаровым, В. А. Образцовым, О. В. Полстоваловым, Н. И. Порубовым и другими специалистами. Современные исследователи, указывая на значимость интернет-ресурсов для получения доказательственной, ориентирующей, вспомогательной информации, комплексно, на основе системного подхода данную проблематику не изучали.

Вопросы, которые рассматривает соискатель, как правило, поднимаются в диссертационных исследованиях, посвященных методике расследования компьютерных и, как сегодня пишут некоторые криминалисты, высокотехнологичных преступлений. Наиболее полно они отражены в трудах В. Б. Вехова, Ю. В. Гаврилина, С. В. Зуева, В. А. Мещерякова, Н. В. Олиндер, В. В. Полякова, Е. Р. Россинской, А. Г. Себякина, А. Б. Смушкина, А. И. Усова, А. Н. Яковлева и других ученых.

Отдельным аспектам использования сети «Интернет» и ее ресурсов при раскрытии, расследовании, предупреждении и пресечении преступлений внимание уделили В. Ф. Васюков, А. Г. Волеводз, Д. В. Воронков, А. И. Гайдин, Е. И. Галяшина, Д. В. Ким, С. Л. Кисленко, А. Н. Колычева, С. И. Кувычков, С. П. Кушниренко, Н. П. Майлис, С. В. Маликов, Л. Н. Масленникова, А. В. Нестеров, А. Л. Осипенко, А. Н. Першин, А. А. Протасевич, Е. А. Русскевич, В. С. Черкасов, М. Ш. Махтаев, А. В. Шебалин, Н. В. Шувалов и другие ученые.

Вместе с тем, несмотря на плодотворную работу научного сообщества, в настоящее время остро ощущается нехватка специализированных междисциплинарных исследований в рассматриваемой сфере. В юридической литературе отсутствуют достаточно полные, отражающие современные потребности следственной практики и достижения в сфере информационных технологий криминалистические алгоритмы использования ресурсов сети «Интернет» при противодействии преступности. Единообразное понимание сущности и специфики тактико-организационных основ данного направления следственной деятельности, предлагаемое автором диссертации, сформулированные на этом базисе практико-ориентированные рекомендации призваны восполнить имеющиеся пробелы.

**Целью** диссертационного исследования является разработка теоретико-прикладных основ и тактико-организационных рекомендаций по использованию сети «Интернет» для получения криминалистически значимой информации при раскрытии, расследовании, пресечении и предупреждении преступлений.

В основе исследования лежит гипотеза, согласно которой сеть «Интернет» может и должна рассматриваться в качестве самостоятельного объекта криминалистического познания, несущего информацию о результатах действий пользователей в виде знаковых следов, а также иную информацию, которая может быть обнаружена, распознана и использована при расследовании преступлений.

Указанная цель и выдвинутая гипотеза обусловили постановку и последовательное решение нижеизложенных **задач**:

— через призму современной парадигмы криминалистической науки определить основные направления использования ресурсов сети «Интернет» при решении отдельных задач расследования преступлений;

— уточнить и систематизировать терминологический аппарат, относящийся к объекту исследования, обозначить пути его интеграции в криминалистическую теорию;

— оценить значимость предлагаемых теоретических положений для развития других частных криминалистических учений;

— выделить основные направления и описать технологии поисково-познавательной деятельности следователя по использованию сети «Интернет» для установления обстоятельств, имеющих значение для уголовного дела;

— сформулировать систему тактико-организационных рекомендаций по установлению личности пользователя сети «Интернет»;

— рассмотреть понятие и виды IP-адресов, определить их значение в процессе расследования преступления, а также изучить способы получения сведений о них;

— определить условия использования при организации расследования таких идентификаторов, как доменное имя, сетевое имя пользователя, электронная подпись, а также их значимость для установления обстоятельств преступления;

— сформулировать особенности использования ресурсов сети «Интернет» при установлении информации о посягательстве, позволяющей квалифицировать содеянное как преступление;

— предложить алгоритм использования ресурсов сети «Интернет» при изучении личности преступника, его розыске и изобличении;

— сформулировать научно обоснованные организационные и тактические принципы реализации рекомендаций, направленных на использование ресурсов сети «Интернет» при проведении отдельных следственных действий;

— определить перспективные направления совершенствования тактики производства отдельных следственных действий, в рамках которых целесообразно использовать ресурсы сети «Интернет» для разумной экономии сил и средств правоохранительных органов в процессе решения общих и частных задач расследования.

**Объектом** исследования являются криминальная деятельность и действия с неявно выраженной криминальной направленностью, отражаемые вовне за счет функционирования аппаратно-программных средств сети «Интернет», а также деятельность органов предварительного расследования по собиранию, оценке, проверке и использованию в доказывании по уголовным делам криминалистически значимой информации, полученной из Интернета.

**Предметом исследования** выступают закономерности общесоциальной и криминальной деятельности в сети «Интернет», а также деятельности органов предварительного расследования по использованию ресурсов сети «Интернет» в целях получения криминалистически значимой информации.

**Методология и методы исследования**. Материалистическая диалектика, будучи всеобщим методом познания, позволила изучить механизмы криминальной деятельности и деятельности по борьбе с преступностью во взаимосвязи и взаимозависимости с правовыми, социальными и технологическими аспектами функционирования сети «Интернет» как платформы для коммуникации в мировом масштабе.

Наряду с диалектическим использовались общенаучные и частнонаучные методы. Например, эмпирический метод применялся при анализе следственной и судебной практики; анализ, синтез — при изучении нормативных правовых актов и научной литературы; индукция, дедукция, аналогия, моделирование — при выявлении закономерностей отражения криминальной деятельности и действий с неявно выраженной криминальной направленностью в сети «Интернет»; интеграция, дифференциация — при решении задач настоящего исследования с опорой на достижения различных наук; метод экспертных оценок — при проверке выдвигаемых по мере продвижения исследования гипотез. Системный подход обеспечил возможность изучения с позиций криминалистики ресурсов сети «Интернет» как комплексного образования. Деятельностный подход позволил выявить особенности использования ресурсов сети «Интернет» при квалификации преступных посягательств, получении информации о лицах, их совершающих или совершивших.

**Теоретическую основу исследования** составили труды таких ученых, как О. Я. Баев, Р. С. Белкин, Л. В. Бертовский, В. Ф. Васюков, В. Б. Вехов, А. Г. Волеводз, Т. С. Волчецкая, А. Ф. Волынский, Д. В. Воронков, Ю. В. Гаврилин, Е. И. Галяшина, В. Д. Зеленский, С. В. Зуев, Е. П. Ищенко, Д. В. Ким, А. Н. Колычева, И. М. Комаров, В. И. Комиссаров, Н. В. Кручинина, В. П. Лавров, Н. П. Майлис, Л. Н. Масленникова, В. А. Мещеряков,

И. П. Можаева, А. В. Нестеров, В. А. Образцов, А. Л. Осипенко, А. Н. Першин, В. В. Поляков, Е. Р. Россинская, Е. А. Русскевич, А. Г. Себякин, С. А. Сумин, А. И. Усов, и других видных специалистов в области криминалистики.

В процессе исследования автор опирался на теоретические знания не только в области юриспруденции (криминалистики, уголовного, уголовно-процессуального права, криминологии и др.), но и наук, объясняющих особенности работы и взаимодействия средств вычислительной техники, функционирования сети «Интернет».

**Нормативную правовую основу исследования** составили положения Конституции Российской Федерации, федеральных законов, указов Президента Российской Федерации, постановлений Правительства Российской Федерации, ведомственных и межведомственных актов по вопросам применения норм уголовного и уголовно-процессуального права, организации судебно-экспертной деятельности в Российской Федерации, а также международно-правовых актов, касающихся работы сети «Интернет».

**Эмпирическую базу исследования** составили результаты анализа судебной, следственной и оперативно-разыскной практики, статистической информации Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации, обзоров практики МВД России, Следственного комитета Российской Федерации.

Соискателем изучены 216 уголовных дел, находившихся в производстве следственных подразделений органов внутренних дел, Следственного комитета Российской Федерации г. Москвы, г. Омска, г. Перми в 2017–2025 гг., в которых ресурсы сети «Интернет» рассматривались как элемент механизма преступления и источник криминалистически значимой информации.

В процессе исследования было проведено анкетирование 184 руководителей следственных органов, следователей и дознавателей Республики Башкортостан, Алтайского края, Пермского края, Приморского края, Ямало-Ненецкого автономного округа, Ленинградской, Московской, Омской, Орловской, Свердловской областей.

Использован личный опыт работы автора в качестве следователя группы по расследованию преступлений, совершенных против собственности, Отделения по расследованию преступлений на территории, обслуживаемой отделом полиции (дислокация — г. Кизел) Межмуниципального отдела МВД России «Губахинский».

**Научная новизна** исследования состоит в разработке тактико-организационных основ использования ресурсов сети «Интернет» при расследовании преступлений. Актуализированы имеющиеся и сформулированы новые теоретические положения и научно-практические рекомендации, а именно:

— выявлены приоритетные направления использования сети «Интернет» при расследовании преступлений, определены научные и практические предпосылки их интеграции в криминалистическую теорию;

— уточнено понятие «идентификатор пользователя сети “Интернет”», раскрывающее его информационную сущность и правовую природу в контексте противодействия преступности;

— предложена классификация пользовательских идентификаторов, определены их криминалистическое значение и особенности установления по ним пользователя как физического лица;

— сформулировано понятие ресурса сети «Интернет» с позиций криминалистики;

— определены тактические и организационные особенности производства отдельных следственных действий, в рамках которых целесообразно использовать сеть «Интернет» для решения общих и частных задач расследования.

**На защиту выносятся следующие основные положения, отражающие новизну диссертационного исследования:**

1. Информационно-телекоммуникационная сеть «Интернет» в силу своего содержания и специфического устройства является самостоятельным объектом познания криминалистической науки — элементом функциональной стороны криминальной и антикриминальной деятельности. Это обусловливает необходимость включения в предметную область криминалистики не только закономерностей применения цифровых технологий при подготовке, совершении

и сокрытии преступлений, но и закономерностей возникновения и отражения следов преступления в информационно-телекоммуникационной сети «Интернет», выявления, фиксации, изъятия и использования данных из интернет-ресурсов для получения криминалистически значимых сведений о преступной деятельности и ее участниках.

2. Сформулировано новое определение понятия «ресурс сети “Интернет”»: это информационная технология, содержащая системно обусловленную, принципиально достижимую с помощью программно-аппаратных средств, потребляемую информацию, способствующую эффективному решению задач расследования преступлений.

Предложена классификация ресурсов сети «Интернет», имеющая значение для отыскания, передачи, получения и использования криминалистически значимой информации: по характеру данных интернет-ресурса (контент, метаданные, сетевые и операторские сведения); по правовому режиму доступа и способу легитимного получения сведений (открытого доступа, условно-открытого доступа, закрытого доступа, анонимизированного/скрытого сегмента); по субъекту владения и управления ресурсом (государственные и муниципальные ресурсы, коммерческие платформы и сервисы, инфраструктурные субъекты интернет-среды, пользовательские (социальные) ресурсы); по функциональному назначению в расследовании (поисково-навигационные, идентификационно-атрибутивные, коммуникационные, транзакционно-финансовые, геоинформационные и мультимедийные, мониторингово-аналитические, профилактические).

На основе данной классификации выделены ключевые направления использования ресурсов сети «Интернет» при расследовании преступлений.

3. С позиций криминалистики раскрыто понятие «идентификатор пользователя “Интернет”» как присваиваемой сетевому подключению или задаваемой пользователем уникальной комбинации символов, позволяющей в процессе раскрытия и расследования преступлений выделять конкретное лицо или оконечное оборудование из неопределенного круга, устанавливать устойчивую

связь между виртуальным образом и реальным субъектом, а также документально фиксировать факты присутствия и выполнения отдельных операций в информационно-телекоммуникационной сети «Интернет».

Предложены система пользовательских идентификаторов и алгоритм действий следователя по получению с их помощью криминалистически значимой информации, необходимой для решения отдельных задач расследования преступлений.

4. Раскрыта сущность тактической операции по использованию ресурсов сети «Интернет» при расследовании преступлений как комплексного криминалистического средства планомерного решения локальных задач расследования, связанных с поиском, фиксацией, проверкой и процессуальным закреплением информации, содержащейся в интернет-ресурсах, хранящейся на программно-аппаратных средствах. Ее специфика обусловливается динамичностью трансформации цифровых объектов, многообразием источников криминалистически значимой информации, рисками утраты данных и ошибок в процессе их интерпретации.

В рамках развития криминалистической теории преодоления противодействия расследованию преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет», разработан алгоритм тактической операции по преодолению анонимности и верификации пользователя Сети.

5. Классифицированы организационные формы использования ресурсов сети «Интернет» при раскрытии и расследовании преступлений, выбор которых обусловливается задачами по обнаружению, фиксации, изъятию, исследованию и использованию криминалистически значимой информации, решаемыми посредством тактических комбинаций и операций.

6. Определены принципы использования интернет-ресурсов при производстве отдельных следственных действий: юридической адресности, двухпоточности действий, тактической оперативности, технологической верифицируемости, технического обеспечения минимизации потери информации,

обеспечения допустимости полученных доказательств, воспроизводимости и проверяемости, объективной обоснованности, рационального выбора тактических приемов.

С опорой на указанные принципы выработана система практико-ориентированных рекомендаций по тактике проведения отдельных следственных действий.

**Теоретическая и практическая значимость диссертационного исследования** заключается в построении внутренне непротиворечивой системы научно и фактически обоснованных положений, совокупность которых позволяет сформулировать практико-ориентированные рекомендации, направленные на оптимизацию процесса использования ресурсов сети «Интернет» при раскрытии, расследовании, пресечении и предупреждении преступлений, а также унификацию правоприменительной практики в условиях цифровой трансформации общества.

Теоретическая значимость исследования заключается в разработке тактико-организационных основ использования ресурсов Интернета при расследовании преступлений. Сформулированные в работе положения, включая категориальный аппарат, необходимы для развития частных криминалистических теорий как основы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей. Некоторые из них уже используются в вузах при актуализации учебной литературы по криминалистике.

Практическая значимость исследования заключается в возможности оперативно повысить без каких-либо материальных затрат эффективность расследования преступлений за счет грамотного использования ресурсов сети «Интернет» в качестве источника криминалистически значимой информации и средства обеспечения результативности отдельных следственных и процессуальных действий. Важно, что изложенные в работе рекомендации могут быть применены в деятельности правоохранительных органов при расследовании большинства категорий уголовных дел.

**Апробация и внедрение результатов исследования.** Основные теоретические положения, выводы, научно-практические рекомендации,

содержащиеся в диссертации, нашли отражение в 28 научных статьях (общий объем — 9,75 п.л.), восемь из которых опубликованы в рецензируемых научных журналах, рекомендованных ВАК при Минобрнауки России для опубликования основных научных результатов диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.

Значительная часть сформулированных диссертантом положений прошла апробацию в ходе конференций, круглых столов и других научных мероприятий: международной научно-практической конференции «Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы» (Москва, 2017); международной научно-практической конференции «Криминалистика: актуальные вопросы теории и практики» (Ростов-на-Дону, 2019); всероссийского научно-практического круглого стола «Вклад Л. Я. Драпкина в криминалистическую науку» (Екатеринбург, 2019); всероссийской научно-практической конференции «Технологии XXI века в юриспруденции» (Екатеринбург, 2019); второй и четвертой международных научно-практических конференций «Технологии XXI века в юриспруденции» (Екатеринбург, 2020 и 2022); международного научно-практического форума «Юридическая наука и образование в эпоху искусственного интеллекта» (Тюмень, 2025); всероссийской научно-практической конференции (с международным участием) «Специальные знания в уголовном процессе» (Москва, 2025); международной научно-практической конференции «Актуальные проблемы правового регулирования, организации и тактики производства следственных действий» (Омск, 2026) и др.

Результаты исследования внедрены в учебный процесс ФГКОУ ВО «Омская академия МВД России» и ФГБОУ ВО «Пензенский государственный университет», в деятельность Отдела МВД России по г. Ноябрьску, следственных подразделений ГУ МВД России по Алтайскому краю и СУ УМВД России по г. Омску.

Отдельные материалы диссертационного исследования, имеющие прикладной характер, используются в мобильном приложении «CrimLib.info —

Справочник следователя», разработанном на базе кафедры криминалистики Уральского государственного юридического университета имени В.Ф. Яковлева в сотрудничестве с Управлением научно-исследовательской деятельности (НИИ криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации и Экспертно-криминалистическим центром МВД России по Свердловской области.

**Структура диссертации** обусловлена целями, задачами, логикой исследования. Работа состоит из введения, трех глав, объединяющих шесть параграфов, заключения, списка литературы и приложений.

# ГЛАВА I. ЗАДАЧИ И НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

## § 1. Сеть «Интернет» как объект изучения криминалистической науки

В современных условиях сеть «Интернет» представляет собой одну из наиболее востребованных технологий: посредством нее обрабатывается большой объем криминалистически значимой информации, необходимой для раскрытия и расследования преступлений. Для одних граждан это инструмент профессиональной деятельности, для других — средство общения и развлечения, для третьих — среда совершения преступления. Учитывая изложенное, можно с уверенностью констатировать, что Сеть выступает новой виртуальной информационной средой, в которой содержатся сведения о лицах, предметах, фактах и событиях. В свою очередь, поиск и изучение таких сведений могут способствовать решению задач уголовного судопроизводства.

Изучение следственной практики и результатов современных исследований в области криминалистики, уголовного права, уголовного процесса позволяет сделать вывод о существовании широкого подхода к пониманию значения сети «Интернет» в поисково-познавательной деятельности следователя. Многочисленные научные публикации последних 10–15 лет являются тому подтверждением[4].

[4] См., например: Гончарова Е. А. Использование сети Интернет в раскрытии и расследовании преступлений // Ученые записки Таврического национального университета имени В.И. Вернадского. Серия «Юридические науки». 2009. Т. 22. № 1. С. 310–315 ; Ишин А. М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета имени И. Канта. Серия «Гуманитарные и общественные науки». 2013. № 9. С. 116–123 ; Развитие информационных технологий в уголовном судопроизводстве / В. С. Балакшин, В. Б. Вехов, В. Н. Григорьев [и др.] ; отв. ред. С. В. Зуев. М. : Юрлитинформ, 2018 ; Родивилин И. П. Использование компьютерной информации при раскрытии и расследовании преступлений, совершенных с использованием сети Интернет // Криминалистика: вчера, сегодня, завтра : сборник научных трудов. Иркутск : Восточно-Сибирский институт МВД России, 2015. С. 173–178 ; Гольцов С. Е. Особенности расследования преступлений, совершаемых с применением средств анонимизации в сети Интернет и мобильной связи // Теория и практика общественного развития. 2023. № 5. С. 165–169 ; Россинская Е. Р. Тренды развития криминалистики в условиях цифровой трансформации современной преступности // Союз криминалистов и криминологов. 2025. № 1. С. 162–173 и др.

Нас интересует научная и практическая проблема использования сети «Интернет» в расследовании преступлений, чтобы в результате ее исследования и разрешения предложить системный подход к применению таких информационных ресурсов при решении конкретных задач расследования.

Семантика слова «использование» (через которое мы определяем предназначение Сети применительно к процессу расследования) предполагает действие или скорее даже *функцию* (выделено нами. — *К. С.*), реализация которой позволяет достичь целей уголовного судопроизводства. Достижение указанных целей системы расследования будет происходить вследствие изменения элементов данной системы за счет внедрения в нее сети «Интернет».

С позиции теории систем функция определяется как способ проявления активности системы, устойчивые активные взаимоотношения вещей, при которых изменения одних объектов приводят к изменениям других[5]. При рассмотрении процесса расследования как динамической системы функция использования необходимых средств будет представлена как свойство, в динамике приводящее к достижению цели, изменению в процессе функционирования состояния системы[6]. Эту функцию система расследования реализует посредством применения комплекса приемов, средств и методов судебного исследования доказательств. Таким образом, сеть «Интернет» выступает плацдармом для использования криминалистических приемов, средств и методов работы, проявление сущности и исследование которых Р. С. Белкин включал в основную часть предмета криминалистики[7].

В связи с тем, что закономерности, составляющие предмет криминалистики, лежат в сфере судебного исследования, т.е. деятельности органов дознания, следствия, суда, экспертных учреждений по установлению истины в процессе судопроизводства, Р. С. Белкин в предмет науки включает закономерности возникновения, собирания, исследования, оценки и использования доказательств[8].

---

[5] Сурмин Ю. П. Теория систем и системный анализ : учебное пособие. Киев : МАУП, 2003. С. 132.
[6] Сурмин Ю. П. Указ. соч. С. 133.
[7] Белкин Р. С. Курс криминалистики. 3-е изд., доп. М. : Юнити-Дана : Закон и право, 2001. С. 61.
[8] Белкин Р. С. Указ. соч. С. 62.

Эта точка зрения и по сей день в криминалистической науке является доминирующей, определяющей основу дефиниций ее предмета для большинства научных школ[9]. В своих фундаментальных трудах ученый акцентирует внимание на том, что термин «доказательство» им используется не в строгом процессуальном значении, поскольку не вся возникающая в процессе совершения преступления информация может приобрести значение доказательства, а при действиях по отысканию и собиранию информация еще не имеет статуса доказательств[10]. Поэтому и мы будем вести речь о возникновении информации о преступлении, собирании, исследовании, оценке и использовании криминалистически значимой информации и доказательств в сети «Интернет», которую в большинстве случаев определяют как глобальную информационную систему, содержащую колоссальные объемы данных[11].

Следует отметить научные труды А. Н. Колычевой. Она рассматривает сеть «Интернет» фактически как следовоспринимающий объект, в котором отображаются электронные следы, но оговаривает отличие процесса электронно-цифрового следообразования от его традиционного представления в криминалистической науке как процесса отражения взаимного действия следообразующего и следовоспринимающего объектов друг на друга[12].

Отсюда с точки зрения предмета нашей работы процессы, реализуемые преступником и иными имеющими отношение к преступлению лицами в сети «Интернет», выступают в качестве элементов материальной и виртуальной обстановки. Они носят следообразующий характер и во многом определяют

---

[9] См.: Гаврилин Ю. В., Головин А. В., Тишутина И. В. Криминалистика в понятиях и терминах : учебное пособие. М., 2006. С. 8 ; Драпкин Л. Я., Карагодин В. Н. Криминалистика : учебник. 2-е изд. М., 2011. С. 3 ; Криминалистика. Углубленный курс / под общ. ред. А. Г. Филиппова. М., 2012. С. 9 ; Меретуков Г. М. Еще раз об объекте и предмете криминалистики // Научный журнал Кубанского государственного аграрного университета. 2014. № 96. С. 633–652 ; Руденко А. В. Проблема определения понятия, предмета и объекта криминалистики // Теория и практика общественного развития. 2014. № 6. С. 171–173 ; Эксархопуло А. А. О предмете криминалистики и его определении // Вестник криминалистики. 2003. Вып. 4 (8). С. 20 и др.

[10] См.: Белкин Р. С. Указ. соч. С. 63.

[11] Основы информационно-библиографической культуры : электронное учебно-методическое пособие НИЯУ МИФИ [Электронный ресурс] // URL: http://library.mephi.ru/icb2/glav5_new.html ; https://www.rsatu.ru/upload/medialibrary/318/Lektsiya-5.pdf (дата обращения: 01.07.2026) и пр.

[12] См.: Колычева А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : дис. … канд. юрид. наук. М., 2018. С. 29–52.

специфику способа совершения преступления. Таким образом, сеть «Интернет» и ее ресурсы становятся объектом изучения криминалистики как специфическая среда, в которой осуществляются действия по подготовке, совершению и сокрытию преступления.

Данное утверждение, безусловно, может быть подвергнуто критике с позиции того, что сеть «Интернет» является реально существующим объектом — информационной средой, изменения в которой выступают результатом реализации преступного способа, а не самим способом.

Тем не менее, если вернуться к вышеуказанному определению сети «Интернет» как глобальной информационной системы, содержащей огромные объемы данных, в которой любой информационный процесс, действие, основанные на принципах, правилах и протоколах функционирования этой системы, приводят к изменению самой системы в части многих ее элементов, дополняя, меняя или удаляя определенные данные, то Интернет становится материализованной средой фиксации преступных действий, наглядно отражающей примененный преступником способ совершения преступления.

Впрочем, с другой стороны, с позиции криминалистического учения о способах совершения и сокрытия преступлений обратное утверждение позволяет рассматривать сеть «Интернет» как внешнюю по отношению к способу систему. Обратимся к другим определениям сети «Интернет»: «Интернет — глобальная информационная система, которая логически взаимосвязана пространством уникальных адресов»[13]. Кроме того, Интернет трактуют как основанное на самых передовых технологиях глобальное информационное пространство[14]. Еще одна дефиниция говорит об Интернете как о «всемирной сети компьютеров, связанных друг с другом с помощью специальных электронных адресов»[15].

---

[13] См.: Батищев П. С. Основы Интернет [Электронный ресурс] // URL: https://psbatishev.narod.ru/internet/12.htm (дата обращения: 01.02.2026).

[14] См.: Основы информационно-библиографической культуры.

[15] См.: Сергеевичева Н. В. Основы самостоятельной и исследовательской работы (КМТ) [Электронный ресурс] // URL: https://edu-apet.ru/course/view.php?id=2535 (дата обращения: 01.02.2026).

24 октября 1995 г. Федеральный сетевой совет (Federal Networking Council) одобрил резолюцию, определяющую Интернет как «глобальную информационную систему, которая:

— логически взаимосвязана пространством глобальных уникальных адресов, основанных на интернет-протоколе (IP) или на последующих расширениях или преемниках IP;

— способна поддерживать коммуникации с использованием семейства протоколов TCP/IP;

— обеспечивает, использует или делает доступными на общественной или частной основе высокоуровневые услуги, надстроенные над описанной здесь коммуникационной и иной связанной с ней инфраструктурой»[16].

Понятие Интернета приводится в Модельном законе об основах регулирования Интернета, принятом 11 мая 2011 г. на 36-м пленарном заседании Межпарламентской ассамблеи государств — участников СНГ. Согласно вышеупомянутому Модельному закону «Интернет — это глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов и протокола передачи данных и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц»[17].

В научной литературе встречается отождествление сети «Интернет» с киберпространством. В частности, на это обращает внимание Д. Е. Добринская: «…очень часто исследователи отождествляют киберпространство и пространство интернета»[18]. Сама же она определяет киберпространство значительно шире — как «пространство функционирования продуктов информационно-коммуникационных

---

[16] Голицына И. Н. Мировые информационные ресурсы : учебно-методическое пособие. Казань : Казанский университет, 2014. С. 12.

[17] Информационный бюллетень Межпарламентской ассамблеи государств — участников СНГ. 2011. № 51. С. 191–198.

[18] Добринская Д. Е. Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18, Социология и политология. 2018. Т. 24. № 1. С. 58.

технологий, позволяющих создавать чрезвычайно сложные системы взаимодействий агентов с целью получения информации, обмена и управления ею, а также осуществления коммуникаций в условиях множества различных сетей»[19].

Профессор В. А. Мещеряков также включает в категорию киберпространства не только сеть «Интернет», но и все электронно-цифровые устройства, используемые людьми. А определяет киберпространство еще шире — как «динамическую среду присутствия человека, состоящую из:

1) информационно-технической инфраструктуры компьютерных систем и их сетей;

2) системы информационно-цифровых объектов, созданных и функционирующих в этой инфраструктуре;

3) системы акторов (пользователей и созданных ими компьютерных программ), использующих информационно-цифровые объекты в инфраструктуре компьютерных сетей для решения целевых задач;

4) установленных правил (протоколов) сетевого взаимодействия всех указанных выше элементов»[20].

С учетом вышеизложенного есть основания говорить, что все перечисленные определения толкуют Сеть через категории, характеризующие место («пространство», «адрес»)[21]. В то же время это место жестко не привязано и не зависит от конкретного пространственно-временного расположения. Взаимодействие в сети «Интернет» не детерминировано жесткой пространственно-временной связью: информационный контакт сторон осуществляется дистанционно и опосредованно, вне зависимости от синхронизации их активности в рамках используемого сетевого ресурса. Безусловно, такое взаимодействие требует со стороны конкретных лиц физического участия, которое может

---

[19] Добринская Д. Е. Указ. соч. С. 59.

[20] Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. С. 53.

[21] См., например: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных путем неправомерного доступа к компьютерной информации или посредством использования электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет")» // Российская газета. № 293. 28.12.2022.

происходить как одномоментно, так и в разное время, но доступно оно может быть им практически в любом географическом пространстве. Как указывает Д. Е. Добринская, «виртуальность здесь не выступает противоположностью действительности, виртуальное место не является местом в привычном смысле, когда место или пространство для взаимодействия ограничено пространственно-временными рамками»[22].

И несмотря на то, что эти пространственные характеристики виртуальны, они по отношению к действиям лиц, использующих сеть «Интернет», выступают категорией места как внешнего фактора, влияющего на выбор того или иного действия и средства. Например, при использовании сети «Интернет» для сбыта или производства наркотических средств возможность бесконтактной передачи наркотиков, прекурсоров, денег без посещения сбытчиком конкретного географического места и без непосредственного физического контакта с покупателем определяет выбор этого способа совершения преступления.

Но этот внешний фактор реализуется в конкретных временны́х условиях, что в совокупности образует категорию обстановки, детерминирующую не только выбор способа действия, но и те пространственно-временные условия, в которых этот способ реализуется, а соответственно, оставляет следы реализации. Поскольку нас интересуют не все осуществляемые в сети действия, а только те, которые лежат в уголовно-правовом поле, то с позиции науки криминалистики эти действия и процессы образуют противоправную деятельность, ее функциональную сторону — систему процессов взаимодействия участников преступления между собой и с материальной средой, сопряженных с использованием соответствующих орудий, средств и иных отдельных элементов обстановки, называемую механизмом преступления[23].

С точки зрения Р. С. Белкина, «элементами системы механизма преступления выступают: 1) субъект преступления; 2) отношения субъекта преступления: к

---

[22] Добринская Д. Е. Указ. соч. С. 64.

[23] См.: Кустов А. М. Теоретические основы криминалистического учения о механизме преступления. М., 1997. С. 15.

своим действиям, их последствиям, к соучастникам; 3) предмет посягательства; 4) способ преступления как система детерминированных действий; 5) преступный результат; 6) место, время и другие обстоятельства, относящиеся к обстановке преступления; 7) обстоятельства, способствующие или препятствующие совершению преступления; 8) поведение и действия лиц, оказавшихся случайными участниками (активными и пассивными) события; 9) связи и отношения между действиями (способом преступления) и преступным результатом, между участниками события, между действиями и обстановкой, субъектом преступления и предметом посягательства и т.п.»[24].

Понятию механизма преступления посвящено достаточно много научных исследований[25], поэтому мы не будем приводить соответствующую научную полемику. Здесь лишь хотим поддержать научную позицию о том, что категория «механизм преступления» относится к конкретному преступному посягательству, с которым сталкиваются субъекты расследования. «Информация о механизме преступления и сопутствующих ему обстоятельствах возникает с момента формирования этого механизма и пополняется в течение всего времени его функционирования»[26]. Познанию механизма преступления способствует другая криминалистическая категория — «криминалистическая характеристика преступления», содержащая обобщенные данные о практически тех же элементах, что и те, которые входят в механизм преступления, собранные на основе анализа уже совершенных и расследованных аналогичных посягательств. Сеть «Интернет» вполне может выступать источником сведений о криминалистической характеристике определенной категории преступлений, особенно совершаемых с использованием Сети или электронно-цифровых технологий. Таким образом, если

[24] Белкин Р. С. Указ. соч. С. 88.

[25] См.: Кустов А. М. Криминалистическая концепция механизма преступления // Вестник МФЮА. 2016. № 2. С. 164–167 ; Зорин Г. А. Теоретические основы криминалистики. Минск : Амалфея, 2000. С. 201 ; Кирсанов З. И. Криминалистические учения в механизме преступления и его расследовании. М., 2004. С. 11 ; Лубин А. Ф. Методология криминалистического исследования механизма преступной деятельности : дис. ... д-ра юрид. наук. Н. Новгород : НЮИ МВД России, 1997 ; Румянцева И. В. Роль криминалистической диагностики механизма преступления в установлении обстоятельств, подлежащих доказыванию // Преступность в Западной Сибири: актуальные проблемы профилактики и расследования преступлений : сборник научных статей. Тюмень : Тюменский государственный университет, 2013. С. 430–434 и др.

[26] Белкин Р. С. Указ. соч. С. 88.

механизм отражает индивидуальную динамику преступного события, то криминалистическая характеристика преступления представляет собой его обобщенную теоретическую модель, выступающую инструментом расследования.

В то же время категория криминалистической характеристики и ее содержание применительно к видам и группам преступлений представляют собой не закономерности преступной деятельности как таковой, а средство ее познания через реализацию деятельности по раскрытию, расследованию и предотвращению преступлений, что относится ко второй части объекта криминалистической науки. Наряду с этим сеть «Интернет» с ее информационным содержанием и технологиями создания, передачи и обработки информации выступает средой восприятия, отражения и сохранения этой информации, становящейся криминалистически значимой в силу связи с конкретным преступлением и процессом расследования. Возможность поиска и фиксации этой информации делает сеть «Интернет» специальным средством, которое в результате адаптации к задачам уголовного судопроизводства трансформируется в систему криминалистических средств и методов.

Помимо информационного поиска в ходе расследования преступлений, сеть «Интернет» реализует и другие функции, позволяющие отнести ее к криминалистическому средству (передача информации, удаленный доступ к объектам оперативного и следственного интереса, дистанционный характер производства следственных действий, определение местоположения значимых для расследования объектов, анализ собранных по делу сведений и пр.).

Таким образом, возможно сделать промежуточный вывод о том, что сеть «Интернет» в силу содержания и специфического устройства является самостоятельным объектом познания криминалистической науки — элементом функциональной стороны криминальной и антикриминальной криминалистической деятельности. Это обусловливает необходимость включения в предметную область криминалистики не только закономерностей применения цифровых технологий при подготовке, совершении и сокрытии преступлений, но и закономерностей возникновения и отражения следов преступления в

информационно-телекоммуникационной сети «Интернет», выявления, фиксации, изъятия и использования данных из интернет-ресурсов для получения криминалистически значимых сведений о преступной деятельности и ее участниках[27].

Приступая к рассмотрению понятия и содержания ресурсов сети «Интернет», следует отметить, что применительно к деятельности следователя, осуществляющего расследование конкретного посягательства, не вся сеть «Интернет» выступает объектом познания, а те ее ресурсы, которые могут содержать криминалистически значимую информацию по находящемуся в его производстве уголовному делу (в том числе сведения, отражающиеся на аппаратно-программных комплексах).

В словарях «ресурс» — это, во-первых, запасы, источники чего-нибудь; во-вторых, средство, к которому обращаются в необходимом случае[28]. Применительно к практике борьбы с преступностью интернет-ресурсы выступают в качестве источников информации, одновременно они служат средством для ее отыскания, получения и обработки.

В Словаре русского языка Института лингвистических исследований Российской академии наук нам особенно подходит отмеченное как устаревшее значение «ресурса» как средства, к которому можно обратиться в затруднительных обстоятельствах, выхода, возможности[29]. Полагаем, что при возможном дефиците криминалистически значимой информации для расследования преступления тот или иной ресурс сети «Интернет» может восполнить этот недостаток в виде ориентирующей или доказательственной информации.

Специфика сети «Интернет» определяет необходимость оперирования категорией «информационный ресурс». Этот термин появился в 1970-е гг. в

---

[27] См. подробно: Белова К. С. Сеть Интернет как объект изучения криминалистической науки // Известия Юго-Западного государственного университета. Серия «История и право». 2024. Т. 14. № 5. С. 105–114.

[28] Толковый словарь Ожегова [Электронный ресурс] // URL: https://slovarozhegova.ru/ (дата обращения: 10.04.2025).

[29] Словарь русского языка : В 4 т. [Электронный ресурс] / РАН, Ин-т лингвистич. исследований ; под ред. А. П. Евгеньевой. 4-е изд., стер. М. : Рус. яз. ; Полиграфресурсы, 1999. URL: https://kartaslov.ru (дата обращения: 01.07.2026).

научных трудах по кибернетике и в дальнейшем получил широкое распространение, выступая в качестве четвертой составляющей экономических ресурсов общества (в дополнение к материальным, трудовым и финансовым). В этом контексте под информационными ресурсами понимается вся совокупность сведений, получаемых и накапливаемых в процессе развития науки и практической деятельности людей, для их многоцелевого использования в общественном производстве и управлении. Эти сведения «отображают естественные процессы и явления, зафиксированные в результате научных исследований и разработок или других видов целенаправленной деятельности в различного рода документах (отчеты о НИР, патенты, массивы данных и т.д.), понятиях и суждениях и др.»[30].

Дальнейшее развитие указанная категория получила в информационных, социально-коммуникационных и библиотечных науках. Не остались в стороне и правоведы. Так, в одном из первых нормативных актов, где для целей правоприменения были даны определения некоторых понятий из области кибернетики, — в Федеральном законе от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» — информационные ресурсы рассматривались как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, базах данных и др.). В этой дефиниции информационный ресурс отождествлялся с официальным источником информации, которым является документ.

Особенность сети «Интернет» в том, что не вся информация в ней может иметь строгую форму с требуемыми для документов реквизитами. Зачастую она хаотична (например, содержание форумов, комментариев в социальных сетях и пр.) и структурирована только по определенным массивам и сервисам. Возможно, по этой причине действующий Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» не содержит

[30] Основы информационно-библиографической культуры.

определения «информационных ресурсов», хотя законодатель оперирует этой категорией (ст. 12.2, 15.3-2, 15.4, 15.8, 15.9).

Еще одну дефиницию информационных ресурсов, характерную для 1990-х гг., находим в ГОСТ 7.0-99 «Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения»: «совокупность данных, организованных для эффективного получения достоверной информации»[31]. Такая конструкция, трактующая нужное нам средство через информацию, организованную для получения другой информации, тавтологична, отражает упрощенный подход к проблеме и не вписывается в структуру субъект-объектной деятельности. С этой точки зрения определение, зафиксированное в ГОСТ Р 7.0.107-2022 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиотечно-информационная деятельность. Термины и определения», является более точным: «Информационный ресурс: данные и/или документы, организованные для получения информации, представленные в любой знаковой системе, на любом физическом носителе и/или распространяемые в информационно-телекоммуникационных сетях»[32].

Сопоставляя дефиниции, зафиксированные в нормативных правовых актах разных лет, нетрудно заметить, что за последние годы ввиду масштаба процессов цифровизации дискуссия о статусе и значении информационных ресурсов вышла на новый уровень. Так, Т. Ф. Берестова полагает, что пришло время для развития самостоятельного научного направления «Информационное ресурсоведение». При этом «информационный ресурс» автором рассматривается как «целенаправленно

---

[31] ГОСТ 7.0-99 «Система стандартов по информации, библиотечному и издательскому делу. Информационно-библиотечная деятельность, библиография. Термины и определения» (утв. постановлением Государственного комитета РФ по стандартизации и метрологии от 07.10.1999 № 334-ст.) [Электронный ресурс] // URL: https://docs.cntd.ru/document/1200004287 (дата обращения: 10.04.2025).

[32] ГОСТ Р 7.0.107-2022 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиотечно-информационная деятельность. Термины и определения» (утв. и введен в действие приказом Росстандарта от 26.05.2022 № 396-ст) [Электронный ресурс] // URL: https://files.omsu.ru/about/structure/science/ub/sibid/%D0%93%D0%9E%D0%A1%D0%A2-%D0%A0-7_0_107-2022.pdf (дата обращения: 10.04.2025).

созданная информация, реализующая инструментальную функцию через ее использование в качестве средства определенного вида деятельности, которая обладает потребительской ценностью, может выступать в качестве товара на информационном рынке»[33]. В данном случае Т. Ф. Берестова акцентирует внимание на функциональном признаке (средство деятельности) и целевом назначении (потребительская ценность), предлагая через указанную дефиницию совокупность неких информационных объектов разделять на подпадающие под предложенное определение, т.е. являющиеся информационными ресурсами, и не подпадающие под него.

В нашем случае к имеющим значение для расследования преступлений ресурсам сети «Интернет» будут относиться те, использование которых позволит получить сведения об обстоятельствах совершенных преступлений либо о причастных к ним лицах, а также решить уголовно-процессуальные и организационно-тактические задачи в ходе предварительного расследования и судебного следствия.

С этой точки зрения, учитывая специфику функционирования сети «Интернет» и организацию процесса расследования, на наш взгляд, утверждать о включаемом в определение Т. Ф. Берестовой признаке — целенаправленном создании информации — можно лишь с определенной оговоркой. По отношению к преступной деятельности, когда злоумышленники используют для достижения противоправных целей сеть «Интернет», уместно говорить о целенаправленном создании в сети фишинговых сайтов, продаже запрещенных предметов на интернет-площадках, организации интернет-казино, публикации запрещенного контента и пр. Но по отношению к деятельности по расследованию преступлений возникновение информации, как правило, не будет целенаправленным, поскольку правоохранительные органы используют уже имеющиеся в Сети данные. Как характеризующий информационный ресурс признак «целенаправленность

[33] Берестова Т. Ф. Информационное ресурсоведение как новое научное направление: постановка проблемы // Научно-техническая информация. Серия 1, Организация и методика информационной работы. 2015. № 7. С. 1–9.

создания» применительно к расследованию преступлений будет иметь место при принятии мер криминалистической профилактики и пресечении преступлений (например, в рамках функционирования АПК «Безопасный город»).

В современной научной литературе выделяют специфические особенности, которыми обладают информационные ресурсы: нерасходуемость/неисчерпаемость, возможность многоразового и многоцелевого использования; постоянный рост объемов; изменчивость состава; различные темпы старения информации, обусловливающие сложность определения ее актуальности; неразрывное единство элементов, составляющих совокупные информационные ресурсы[34].

Эти особенности являются условиями работы правоприменителя с информационными ресурсами и могут рассматриваться как в позитивном, так и в негативном ключе. Так, специфика, связанная с нерасходуемостью и возможностью многократного использования, позволяет неоднократно обращаться к ресурсу для получения сведений о преступном деянии. Например, при производстве судебной компьютерной экспертизы данные о времени публикации записи на ресурсе позволяют установить хронологию преступного события и сопоставить виртуальные следы. В то же время возможность внесения изменений в источник сведений, наоборот, оказывает отрицательное воздействие на объективность поисково-познавательной деятельности следователя, поскольку порождает риски уничтожения или модификации доказательственной информации.

В логических системах (к разновидности которых относится процесс расследования преступлений) ресурс наделяется взаимообусловленными конститутивными признаками: «системная обусловленность, принципиальная достижимость, потребляемость (способность расходоваться), эффективность»[35].

---

[34] Основы информационно-библиографической культуры.

[35] Ладушкин С. И. Ресурс как проблема логики [Электронный ресурс] // Проблемы современной науки и образования. 2015. № 1 (31). URL: https://cyberleninka.ru/article/n/resurs-kak-problema-logiki/viewer (дата обращения: 30.05.2025).

Процесс расследования выступает по отношению к интернет-ресурсу потребляющей системой, а сеть «Интернет» — снабжающей, содержащей потребляемый пользователем ресурс, обеспечивающий получение криминалистически значимой информации. В качестве потребляющей подсистемы субъект расследования самостоятельно определяет вид и объем требуемого ресурса и необходимых сведений для разрешения тактических задач на определенном этапе расследования. При этом следователь не просто воспринимает сеть «Интернет» как статичное системное образование, состоящее из информационных источников и технологий функционирования информации. Для целей расследования принципиальное значение имеет понимание того, как элементы сетевой инфраструктуры взаимодействуют между собой, отражаются во внешнем мире и — главное — как использовать данные сведения для решения задач расследования.

Реализация указанного подхода обусловлена принципиальной достижимостью криминалистически значимой информации на ресурсах сети «Интернет», которая выражается в относительной доступности информации из Сети. Из данного положения вытекают важные логические следствия, определяющие природу поисково-познавательной деятельности в процессе расследования. Она может осуществляться следователем как непосредственно (с опорой на собственные навыки), так и путем привлечения лиц, обладающих специальными знаниями. Данное положение всецело относится к сети «Интернет». Даже когда речь идет о сети ограниченного доступа, каковой является «Даркнет», эта система становится принципиально доступной при задействовании необходимых специальных познаний, позволяющих получить криминалистически значимую информацию, в том числе доказательственную[36].

Таким образом, сущность принципа потребляемости ресурсов сети «Интернет» выражается в целевом и конкретном применении полученных сведений для решения задач расследования. Использование потенциала сети

[36] Романова Л. И., Дремлюга Р. И. Преступный мир Darknet // Юридическая наука и практика. 2018. Т. 14. № 1. С. 52–60.

«Интернет» ориентировано на выполнение традиционных задач расследования (розыск, идентификация и пр.), но на качественно ином уровне оперативности, с минимальной затратой сил и средств, а также в дистанционном формате.

В данном контексте ключевое значение приобретает принцип эффективности, суть которого заключается в обеспечении решения поставленных задач в максимально короткие сроки при наименьших затратах трудовых, материальных и финансовых ресурсов[37].

Таким образом, под используемыми в расследовании информационными ресурсами мы будем понимать системно обусловленную, принципиально достижимую, потребляемую и эффективную информацию, способствующую установлению наличия или отсутствия обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для дела.

Впрочем, нас интересует не просто информационный ресурс, а ресурс в сети «Интернет».

Этимология выражения «интернет-ресурс» восходит к специальной компьютерной терминологии, где в информационных технологиях системным ресурсом называют физический или виртуальный компонент ограниченной доступности в компьютерной системе. К физическим компонентам относят части компьютерной системы (например, элементы памяти и т.п.), к виртуальным — файлы. «Именно к виртуальной части ресурсов восходит идея веб- (интернет-)ресурсов. В эпоху молодого Интернета в сети искали документы, а точнее файлы, которые имели специальный адрес. Вскоре под ресурсом в Интернете стали также понимать и связанную в сеть всю информационную систему (например, электронные библиотеки и т.п.)»[38].

Сегодня интернет-ресурс (синонимы: «веб-ресурс», «веб-сайт», «веб-сервис», «сайт») определяется как совокупность интегрированных средств

---

[37] См., например: Волынский А. Ф. Эффективность как принцип организации предварительного расследования преступлений // Вестник Московского университета МВД России. 2016. № 4. С. 27–32.

[38] Глоссарий интернет-маркетинга [Электронный ресурс] // URL: https://www.glossary-internet.ru (дата обращения: 10.04.2025).

программно-аппаратного характера, а также информации, предназначенной для публикации в сети «Интернет», которая может содержать материалы в текстовой, графической и мультимедийной форме[39]. В другом источнике под информационными ресурсами Интернета понимается вся совокупность информационных технологий и баз данных, которые доступны при помощи этих технологий[40].

Согласно ГОСТ Р 52872-2019 «Национальный стандарт Российской Федерации. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности» под интернет-ресурсом понимается адресуемый уникальным идентификатором поставщик контента, доступный через сети передачи данных ограниченному или неограниченному числу пользователей[41].

Таким образом, интернет-ресурс характеризуется тремя составляющими: это место размещения информации; информацию принимают, обрабатывают, накапливают, хранят и рассылают с помощью определенных программно-аппаратных средств сервисы, службы, объединенные в специальные информационные технологии; информация в совокупности с указанными технологиями становится источником запрашиваемых сведений.

В отличие от работы с традиционными документальными источниками, где информация неотделима от физического носителя, при поиске интернет-ресурса сетевые протоколы определяют лишь его сетевой адрес, в то время как физическое местонахождение сервера требует дополнительных криминалистических усилий.

---

[39] Глоссарий интернет-маркетинга.

[40] Краткая характеристика ресурсов Интернета [Электронный ресурс] // URL: https://opengl.org.ru/informatsionnye-sistemy-i-tekhnologii-v-zkonomike/kratkaya-kharakteristika-resursov-interneta.html (дата обращения: 10.04.2025).

[41] ГОСТ Р 52872-2019 «Национальный стандарт Российской Федерации. Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности» (утв. и введен в действие приказом Росстандарта от 29.08.2019 № 589-ст). М. : Стандартинформ, 2019.

Это адрес — унифицированный указатель ресурса (Uniform Resource Locator, URL). При запросе информации пользователь получает все адреса, где находятся могущие представлять для него интерес ресурсы, после чего сам выбирает, откуда черпать информацию[42].

Подводя промежуточный итог, необходимо подчеркнуть: применительно к использованию в уголовном судопроизводстве ресурс сети «Интернет» можно определить как информационную технологию, содержащую системно обусловленную, принципиально достижимую с помощью программно-аппаратных средств, потребляемую информацию, способствующую эффективному решению задач расследования преступлений.

Информационные технологии, структурирующие в Сети всю имеющуюся информацию в определенные информационные массивы, по-разному определяются и подразделяются специалистами, в связи с чем в специальных источниках существуют различные классификации интернет-ресурсов[43]. Разрешая задачу нашего исследования, мы рассмотрели имеющиеся подходы по существу и обобщили их.

Не вдаваясь в анализ категорий информационно-технических сфер деятельности, выделим структурные элементы сети «Интернет», содержащие требуемые для расследования ресурсы:

1) электронная почта (e-mail) является старейшим ресурсом сети «Интернет», т.к. появилась еще до ее возникновения и служила для обмена сообщениями между локальными пользователями компьютера. Услуга обмена документами и сообщениями между пользователями оказалась настолько востребованной, что е-

---

[42] Основы информационно-библиографической культуры.

[43] См., например: Бачило И. Л. Информационное право : учебник для вузов. 5-е изд., перераб. и доп. М. : Юрайт, 2026 ; Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки. Волгоград : ВА МВД России, 2008 ; Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001 ; Россинская Е. Р. Криминалистическая теория и практика в условиях цифровизации : монография. М. : Норма, Инфра-М, 2025 и др.

mail стал одним из ключевых приложений, стимулировавших развитие раннего Интернета[44].

В связи с этим данный ресурс чаще всего используется при решении отдельных задач расследования. В частности, анализ списка рассылки, копий сообщений и вложений помогает установить круг общения подозреваемого, связанный с планированием или сокрытием преступления. Письма могут содержать прямые указания на готовящееся преступление, договоренности о его совершении, описание действий или иные значимые детали.

Например, согласно приговору Иркутского районного суда от 23.09.2024 № 1-19/2024 1-364-2023 по делу № 1-19-2024 обвиняемый похитил денежные средства, обещая поставить оборудование для майнинга. В качестве доказательства обмана суд использовал переписку, в которой подсудимый с электронной почты отправлял потерпевшему поддельные договоры на его почту[45].

В другом деле (приговор Курганского городского суда от 04.02.2024 № 1-24/2023 1-695/2022 1-9/2024 по делу № 1-24/2023) был произведен осмотр электронных ящиков после выемки из ООО «Мэйл.Ру» переписки, в которой соучастники преступления согласовывали макеты, логотипы произведений и детали незаконного тиража[46];

2) информационная сеть WWW (World Wide Web), или Всемирная паутина, является самым популярным ресурсом сети «Интернет» и предоставляет удобный доступ к большинству его информационных архивов. Это распределенная гипертекстовая информационная система, содержащая огромное количество (свыше миллиарда) мультимедийных документов, отличительной особенностью которых является возможность ссылаться друг на друга. «Это означает присутствие в текущем документе ссылки, реализующей переход на любой документ WWW, который физически может быть размещен на другом компьютере сети “Интернет”. Информация в WWW представляется в виде документов, каждый из которых

---

[44] См.: Робачевский А. М. Интернет изнутри: Экосистема глобальной Сети. М. : Альпина Паблишер, 2015. С. 185.

[45] URL: sudact.ru/regular/doc/IMfH34xgGRLK/ (дата обращения: 29.06.2026).

[46] URL: sudact.ru/regular/doc/mwKQW3OWCEb5/ (дата обращения: 29.06.2026).

может содержать как внутренние перекрестные ссылки, так и ссылки на другие документы, хранящиеся на том же самом или на любом другом сервере»[47].

В рассматриваемом ресурсе существует большое количество разного рода каталогов, позволяющих ориентироваться в Сети, и несколько способов передачи данных (протоколов), среди которых наибольшей популярностью пользуется протокол передачи гипертекста — http (Hypertext Transfer Protocol). Система универсальных адресов дает возможность присвоить адрес практически всем информационным ресурсам глобальной Сети.

Опираясь на эти базовые механизмы адресации и передачи данных, правоохранительные органы осуществляют фиксацию виртуальных следов. Так, например, при осмотре места происшествия, обыске или осмотре предметов фиксируется содержимое конкретных интернет-страниц, доступ к которым осуществляется по протоколам HTTP/HTTPS на основе их уникальных универсальных адресов. В материалах уголовных дел довольно часто при осмотре интернет-страницы[48] описываются сетевой адрес (URL), который отсылает к конкретному ресурсу, текстовое и визуальное содержимое, а также метаданные и лог-файлы, фиксирующие дату создания, изменения информационных данных на ресурсе[49];

3) электронные доски объявлений BBS (от Bulletin Board System — «система досок объявлений»). По аналогии с газетами или обычными досками объявлений на электронных досках размещаются объявления, рассылаемые пользователями всем, кто их прочитает. На базе электронных досок объявлений и других специальных пакетов можно организовывать совещания, конференции для

---

[47] Основы информационно-библиографической культуры.

[48] См., например: Сидорова К. С. Тактические особенности осмотра интернет-страницы в ходе расследования преступлений // Проблемы криминалистической науки, следственной и экспертной практики : сборник научных трудов / пред. редкол. Я. М. Мазунин. Вып. 11. Омск : Омская академия Министерства внутренних дел РФ, 2021. С. 53–56.

[49] См., например: согласно приговору Новосергиевского районного суда Оренбургской области от 29.07.2021 № 1-39/2021 по делу № 1-39/2021 был произведен осмотр интернет-страницы пользователя, в ходе которого зафиксировано, что фотография аккаунта изменена, а общий доступ к нему закрыт (URL: sudact.ru/regular/doc/bjmZ7Kxw5Q6t/ (дата обращения: 29.06.2026)).

одновременного участия несколько человек с их рабочих мест в разных городах и странах.

Например, «Ф. в период с сентября 1997 года по 10 марта 1998 года, используя свой домашний персональный компьютер Packard Bell 486-CX-33, модем US-Robotics и телефон, зарегистрированный на Екатеринбургской ГТС, находящиеся по адресу его фактического проживания, а также установленную им специализированную компьютерную программу Maximus 3.00 (BBS — Bulletin Board Sistem — электронную доску объявлений), обеспечивающую работу компьютера с удаленными пользователями через телефонную сеть, распространял программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Для этой цели Ф. во второй половине августа 1997 года самостоятельно установил на своем персональном компьютере программное обеспечение «Максимус 3.00» (Maximus 3.00) для обеспечения работы BBS, предназначенной для получения информации с персонального компьютера, где установлена BBS, удаленными пользователями, для общения между ними и администратором, для пересылки электронной почты. Для получения доступа к BBS пользователь должен иметь некоторые начальные познания о персональном компьютере, компьютер, модем и выход на телефонную линию»[50];

4) системы телеконференций, например Usenet, который также построен по принципу электронных досок объявлений и в котором любой пользователь может разместить информацию в одну из групп новостей. Размещенная информация становится доступной всем подписанным на данную группу новостей пользователям.

Системы телеконференций, такие как Usenet, чаще всего фигурируют в преступлениях как инструмент для осуществления нелегальных действий в сети «Интернет» анонимным способом. В судебной практике множество прецедентов

[50] Уголовное дело № 176709 (г. Екатеринбург) по обвинению Ф. в совершении преступления, предусмотренного частью 1 ст. 273 УК РФ.

связаны как непосредственно с Usenet (на международном уровне), так и с ее российскими аналогами — электронными досками объявлений на различных ресурсах. Например, кража, способом совершения которой являлась рассылка фишинговых сообщений для получения доступа к банковским картам[51], размещение на форумах и досках объявлений пошаговых инструкций по бесконтактному сбыту запрещенных веществ, изготовлению оружия и т.д.;

5) система файловых архивов FTP (от File Transfer Protocol — «протокол передачи файлов») — это огромное распределенное хранилище всевозможной накопленной за последние десятилетия в Сети информации и система пересылки файлов. Его создали в 1971 г., чтобы быстро и удобно передавать файлы с одного компьютера на другой и управлять удаленными серверами[52]. Ресурс позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер. Кроме этого, возможен режим передачи файлов между серверами хранилищ.

Архивы FTP содержат терабайты информации. Кроме программ в FTP-архивах можно найти стандарты Интернета RFC (Request for Comments), пресс-релизы, книги по различным отраслям знаний и многое другое. Практически любой архив строится как иерархия каталогов. Многие архивы дублируют информацию из других архивов (так называемые зеркала (mirrors)). Чтобы получить искомую информацию из какой-либо удаленной точки мира, можно найти зеркало где-нибудь в ближайшем регионе и с помощью специальной программы Archive, которая позволяет просканировать FTP-архивы, отыскать тот материал, который будет устраивать пользователя по составу программного обеспечения и коммуникационным условиям[53];

6) информационные системы, например Gopher. Последний был разработан для облегчения поиска нужных серверов в сети «Интернет». Его структура и

---

[51] Суд рассмотрит дело о легализации средств через сайты знакомств и фишинг [Электронный ресурс] // URL: https://rapsinews.ru/judicial_news/20250129/310587639.html (дата обращения: 01.07.2026).

[52] См.: Зверев Д. Протокол FTP: что это такое и как с ним работать [Электронный ресурс] // URL: https://skillbox.ru/media/code/protokol-ftp-chto-eto-takoe-i-kak-s-nim-rabotat/ (дата обращения: 01.07.2026).

[53] См.: Краткая характеристика ресурсов Интернета.

функционал базируются на идее иерархических каталогов. Внешне Gopher выглядит как огромная файловая система, которая расположена на машинах Сети. Первоначально он задумывался как информационная система университета с информационными ресурсами факультетов, кафедр, общежитий и т.п. До сих пор основные информационные ресурсы системы сосредоточены в университетах. Gopher был не только самостоятельным ресурсом, но и перевалочным пунктом для других частей Интернета. Если в Gopher чего-то не было, через Gopherspace возможно было выйти в Сеть, или на FTP-сервер, или в новостную группу и найти там нужный контент[54]. Gopher считается простой системой, легкой в установке и администрировании, достаточно надежной и защищенной. В России Gopher-серверы не так распространены, как во всем мире;

7) информационные ресурсы, например LISTSERV — сервис для обслуживания пересылки электронной почты и управления системами ее адресов. Этот ресурс очень популярен в глобальных компьютерных сетях, поскольку позволяет общаться пользователям, объединенным в группы по интересам. Сервис дает возможность найти интересующую группу, присоединиться к ней и активно участвовать в ее функционировании. LISTSERV во многом пересекается с Usenet, однако это не мешает существованию как одной, так и другой системы[55];

8) каталоги X.500 — это европейский стандарт для компьютерных справочных служб. Они предоставляют централизованную информацию обо всех поименованных объектах Сети (ресурсах, приложениях и пользователях). Ресурс содержит сведения о пользователях Сети, их электронных и обычных адресах, идентификаторах и реальных именах, должностях, местах работы, данные об организациях, описания основных направлений их деятельности[56];

9) справочные службы, например WHOIS — ресурс, который предоставляет доступ к информации обо всех зарегистрированных доменах в сети «Интернет».

---

[54] См.: Голованов В. Gopher, конкурент WWW из 90-х, который пока не стоит списывать со счетов [Электронный ресурс] // URL: https://habr.com/ru/articles/581692/ (дата обращения: 01.07.2026).

[55] См.: Семенов Ю. А. Серверы подписки (LISTSERV) [Электронный ресурс] // URL: http://book.itep.ru/4/45/list_459.htm (дата обращения: 01.07.2026).

[56] См.: Краткая характеристика ресурсов Интернета.

Данная служба аналогична по назначению системе X.500, однако работа с WHOIS отличается от работы с X.500 в силу ее организации. WHOIS — распределенная система, поэтому запросы отправляются по всему множеству серверов WHOIS в сети «Интернет», если только не указан адрес конкретного сервера. В базе данных WHOIS можно получить доступ к следующей информации о домене: DNS-серверы домена, данные о регистраторе, статус домена, даты его регистрации и ее окончания, имя владельца домена[57].

На основании результатов изучения материалов уголовных дел можно сделать вывод о том, что довольно часто следователи получали из данного ресурса массив криминалистически значимой информации: определение провайдера по конкретному соединению, установление владельца сайта, сведения о регистрации доменного имени и т.д. Затем, исходя из полученной информации, направлялись необходимые запросы о получении дальнейших относящихся к расследованию сведений[58];

10) система TRICKLE выступает как доступ по почте к архивам RTF, организованный через специальный шлюз. Этот шлюз имеет навигационные средства для поиска нужной информации в Сети, пользователь может вести с ним своеобразный диалог по почте, выбирая нужную информацию путем ввода специальных команд TRICKLE[59].

Криминальный аспект задействования данных шлюзов состоит в получении анонимного доступа к нелегальному контенту, обходе различных блокировок, управлении кибератаками;

11) протоколы для удаленного доступа к ресурсам (например, Telnet) — одна из самых старых информационных технологий сети «Интернет». Она входит в

---

[57] См.: Что такое WHOIS [Электронный ресурс] // URL: https://handyhost.ru/help/term/chto-takoe-whois.html#:~:text(дата обращения: 01.07.2026).

[58] Здесь и далее приводятся обобщенные результаты проведенного автором анкетирования 184 руководителей следственных органов, следователей, дознавателей Республики Башкортостан, Алтайского края, Пермского край, Приморского края, Ямало-Ненецкого автономного округа, Ленинградской, Московской, Омской, Орловской, Свердловской областей, а также изучения 216 уголовных дел, находившихся в производстве следственных подразделений органов внутренних дел, Следственного комитета РФ г. Москвы, г. Омска, г. Перми в 2017–2025 гг., выраженные в процентном соотношении.

[59] См.: Краткая характеристика ресурсов Интернета.

число стандартов, которых насчитывается три десятка на полторы тысячи рекомендуемых официальных материалов Сети — RFC[60]. Основная функция ресурса — соединение с удаленным портом и установление интерактивного канала связи для передачи команд или получения данных. Протокол Telnet, созданный на основе транспортного протокола TCP, позволяет передавать на удаленный сервер простые текстовые команды для ручного управления процессами и включения взаимодействия между ними. Указанная программа универсальна: она способна работать с различными протоколами[61]. Основная суть использования этих протоколов состоит в том, что они позволяют производить неправомерный доступ к серверам, изучать их содержимое и осуществлять перехват конфиденциальных данных;

12) самостоятельным интернет-ресурсом является совокупность различных мессенджеров и социальных сетей.

Например, Верховный Суд РФ рассматривал кассационную жалобу двух фигурантов. Один из них настаивал: он просто общался в Telegram с коллегами и родственниками, а не использовал мессенджер для преступлений. Суд отклонил этот довод. Экспертиза показала: на устройствах фигурантов был создан отдельный аккаунт. В папках хранились карты с «закладками» (тайниками с наркотиками), реклама интернет-магазина, информация о трудоустройстве «закладчиков». Из переписки следовало, что один из осужденных выполнял роль куратора: координировал продавцов, передавал данные о местах сокрытия веществ. Дополнительно подтвердили картину показания сотрудника силовых структур, который в рамках оперативно-разыскных мероприятий вел переписку с участниками группы: после задержания ответы прекратились. Суд счел, что совокупность доказательств подтверждает: мессенджеры и соцсети использовались для организации и координации преступной деятельности, и это

[60] См.: Краткая характеристика ресурсов Интернета.

[61] См.: Трасковский А. Как пользоваться telnet [Электронный ресурс] // URL: https://timeweb.com/ru/community/articles/kak-polzovatsya-telnet (дата обращения: 01.07.2026).

стало основанием для сохранения квалифицирующего признака «с использованием информационно-телекоммуникационных сетей»[62];

13) электронные торговые площадки (агрегаторы товаров и услуг, маркетплейсы).

Например, согласно сведениям из приговора Вахитовского районного суда г. Казани от 18.07.2023 № 1-198/2023 1-720/2022 по делу № 1-198/2023, фигуранты использовали уязвимость в системе «Портал поставщиков» на площадке Wildberries. Они продавали цифровой контент (например, готовые программные решения, текстовые файлы) при условии полной предоплаты через ввод реквизитов банковской карты. Но система не проверяла, действительны ли карты и есть ли на них деньги. Если карта оказывалась нерабочей или средств не хватало, система всё равно формировала отчет о продаже. На основании этих ложных данных площадка переводила деньги от продажи цифрового контента на счет поставщика (за вычетом комиссии площадки). Следствие изучило лог-файлы системы, данные о транзакциях и выявило схему: преступники искусственно создавали отчеты о продажах, чтобы выводить средства. В приговоре подробно разбиралось, как именно действовала автоматизация, какие технические моменты позволили схеме сработать и какие доказательства (лог-файлы, отчеты) легли в основу обвинения[63].

Как правило, из перечисленных ресурсов следователю (если у него нет технического образования) известны три-четыре (87 % опрошенных), еще меньшее количество ресурсов непосредственно используется. Эта тенденция имеет место и в практике обращения к информационно-поисковым системам, применение которых позволяет искать нужную информацию на обозначенных интернет-ресурсах[64].

---

[62] ВС включил мессенджеры в инструменты совершения киберпреступлений [Электронный ресурс] // URL: https://rapsi-pravo.ru/judicial_analyst/20230914/309217921.html (дата обращения: 01.07.2026).

[63] URL: https://sudact.ru/regular/doc/HoDtGgBkPkQu/?ysclid=mqt9cip21r903223101 (дата обращения: 01.07.2026).

[64] См.: Белова К. С. Понятие и виды ресурсов сети Интернет, обращение к которым возможно в процессе расследования преступлений // Эксперт-криминалист. 2026. № 1. С. 26–29 ; Малахов А. С., Сидорова К. С. Обнаружение сведений о криминальных событиях с использованием интернет-поисковых систем при раскрытии и расследовании преступлений [Электронный ресурс] // 100 лет уголовному розыску России: история, современность, перспективы : материалы всероссийской научно-практической конференции, Санкт-Петербург, 8 ноября 2018 г. / сост. М. Л. Родичев. СПб. : Санкт-Петербургский университет МВД России, 2018. С. 102–106. 1 электрон. опт. диск.

Отдельно следует сказать о нейросетях, которые нельзя назвать просто поисковыми системами. В отличие от вышеуказанных систем нейросети обладают значительно большей скоростью поиска. Нейросеть выдает готовый ответ по запросу, а не ресурсы, сайты, содержащие близкую к теме запроса информацию. Поиск ведется как по текстовым массивам данных, так и с обработкой голосовых, аудио- и видеофайлов. Нейросети функционируют как генеративные модели искусственного интеллекта, способные создавать синтетический контент, что трансформирует классический механизм следообразования и порождает проблему верификации достоверности электронных доказательств. Среди наиболее известных нейросетей можно указать GigaChat, You.com, Andi, Perplexity AI, Komo AI, Scite, Consensus, ChatGPT, DeepSeek, Felo AI, Waldo Search, iAsk, Copilot, «Яндекс Нейро».

В одном из дел оперуполномоченный расследовал уличную кражу. Он получил скриншот лица подозреваемого с камеры «Безопасного города», увеличил его и загрузил в аппаратно-программный комплекс «Купол» с нейроаналитикой. Система просканировала тысячи камер по городу, нашла совпадения и помогла составить ориентировку. В результате подозреваемого задержали. В приговоре это отразили так: «личность подсудимого установил аппаратно-программный комплекс “Купол” с функцией нейроаналитики»[65].

Поскольку в связи с перманентным изменением и развитием информационного пространства невозможно предложить исчерпывающий список ресурсов сети «Интернет» и обеспечить актуальность такого описания, целесообразно их классифицировать, выделив значимые для использования в процессе расследования основания. Каждое основание должно создавать понимание у правоприменителя о направлениях и порядке действий при обращении к ресурсу с целью отыскания, передачи, получения, фиксации и использования криминалистически значимой информации.

[65] AI в законе: суды в России оценивают искусственный интеллект как естественный [Электронный ресурс] // URL: https://www.fontanka.ru/2025/12/14/76171234/ (дата обращения: 01.07.2026).

Зачастую у следователя выражение «интернет-ресурс» ассоциируется с конкретным сайтом, на странице которого отражена искомая информация. Однако следует учитывать, что, помимо контентной страницы, явно отражающей значимые для расследования сведения, нужно учитывать инфраструктуру ресурса (включая платформы, сайты, аккаунты, облачные кабинеты, коммуникационные и транзакционные интерфейсы, а также элементы доменной и сетевой инфраструктуры), без которой невозможна атрибуция субъекта преступной деятельности или иных участников расследования. Тем самым характер данных интернет-ресурса — контент, метаданные, сетевые и операторские сведения — выступает одним из первых и значимых оснований классификации.

Для методики расследования принципиально выделить тип данных, извлекаемых из ресурса:

— контентные данные — тексты, изображения, видео-, аудиофайлы, публикации, комментарии, карточки товаров/услуг, элементы интерфейса транзакций;

— метаданные — сведения о времени, идентификаторах, параметрах файла, связи объекта с аккаунтом/устройством, журнальные отметки о редактировании/удалении, хеш-значения и др.;

— сетевые и операторские данные — сведения о соединениях, трафике, платежах, идентификаторах оборудования и абонента, формируемые в системах связи. В Федеральном законе от 07.07.2003 № 126-ФЗ «О связи» описывается состав сведений абонентских баз, включая данные о соединениях, трафике и платежах, позволяющие идентифицировать абонента или оконечное оборудование.

Выделенные группы данных наглядно демонстрируют, что недостаточно установить и зафиксировать контент, содержание которого может выглядеть убедительным для целей доказывания. Параллельно должны быть обнаружены и получены метаданные и инфраструктурные сведения, которые в совокупности с контентом установят доказываемое обстоятельство, исключив попытки опровержения обвинительного тезиса ссылками на фальсификации или действия иных лиц.

Кроме того, в силу различных правовых режимов доступа к ресурсам следователь не всегда самостоятельно и напрямую в реальном времени может получить требуемую информацию. Отсюда значимо подразделить интернет-ресурсы по правовому режиму доступа и способу легитимного получения сведений.

1. Ресурсы открытого доступа (OSINT-сегмент (от Open Source Intelligence)).

К ним относятся сайты и страницы, доступные без специальных прав (публичные профили, открытые каналы, открытые реестры, публикации организаций, открытые базы судебных актов и т.п.). Информация из этих ресурсов извлекается без преодоления технических средств защиты и без обращения к закрытым учетным данным. При этом даже открытость не снимает требований к корректной фиксации, поскольку контент динамичен и легко модифицируется или удаляется. Поэтому при выявлении значимой информации ключевым становится своевременное документирование факта ее существования с учетом первого основания классификации.

2. Ресурсы условно-открытого доступа.

Доступ предоставляется после регистрации/авторизации, иногда после подтверждения личности или подписки. Здесь можно выделить две ситуации:

а) следователь получает доступ законно через предоставление данных самим владельцем аккаунта (добровольность);

б) сведения запрашиваются у владельца ресурса (платформы/сервиса) в предусмотренном порядке или извлекаются посредством следственных действий.

3. Ресурсы закрытого доступа.

К ним относятся операторские базы, данные провайдеров, журналы доступа, биллинговые системы, внутренние интерфейсы управления сервисом, облачные хранилища и др. Их специфика заключается в том, что следователь фактически обращается не к странице в Интернете, а к организованным массивам данных о соединениях, трафике, платежах, идентификаторах оборудования и т.п., которые формируются в силу функционирования услуг связи.

4. Ресурсы анонимизированного/скрытого сегмента (darknet-инфраструктуры, сети анонимизации).

К ним относят площадки, функционирующие через анонимизирующие технологические решения, где затруднены идентификация владельца и локализация серверной инфраструктуры. Здесь значимы сбор технических и поведенческих признаков; мониторинг; комбинирование следственных действий и оперативно-разыскных мероприятий; международное взаимодействие. Отнесение к этой группе диктует иные требования к оценке надежности данных: необходимо заранее учитывать высокую вероятность фальсификации.

Не только правовой режим доступа определяет порядок обращения к ресурсу и получение из него информации. Для решения этих задач важно также определить субъекта владения и управления ресурсом. По этому основанию можно выделить:

1) государственные и муниципальные ресурсы — официальные сайты, порталы, реестры, информационные системы органов власти. Их особенности: чаще выраженная юридическая значимость опубликованных сведений, относительно стабильные правила хранения и публикации, более предсказуемые механизмы получения подтверждений и заверенных копий;

2) коммерческие платформы и сервисы — маркетплейсы, сервисы объявлений, банки, службы доставки, агрегаторы услуг. Здесь важно учитывать корпоративные политики хранения данных, регламенты выдачи информации и юрисдикцию владельца;

3) инфраструктурные субъекты интернет-среды — регистраторы доменных имен, хостинг-провайдеры, провайдеры, операторы связи. Отдельно укажем WHOIS-сервисы как инструмент первичной атрибуции доменной регистрации (дата регистрации, сведения о домене и др.), при этом сами по себе данные WHOIS обычно служат ориентирующей информацией и требуют последующей верификации через официальные ответы регистратора;

4) пользовательские (социальные) ресурсы — социальные сети, мессенджеры, форумы, видеохостинги, игровые сообщества, особенностями которых выступают высокая динамичность контента, значимость метаданных, а

также зависимость информации от настроек приватности, алгоритмов выдачи и геолокационных ограничений.

Анализ криминалистической литературы по вопросам расследования преступлений, совершенных с использованием интернет-технологий, позволяет говорить, что авторы хотя и не классифицируют интернет-ресурсы, но рассматривают их преимущественно с позиции информационно-следового подхода, раскрывая места локализации виртуальных следов, или тактико-процессуального подхода, предполагающего описание интернет-ресурсов применительно к тактике определенного следственного действия, позволяющего обнаружить, зафиксировать и изъять искомую информацию. Однако, помимо отыскания криминалистически значимой информации, ресурсы сети «Интернет» могут выполнять обеспечивающую расследование функцию, что также необходимо учитывать в классификации. Здесь ресурсы могут быть сгруппированы по функциональному назначению в расследовании: поиск, идентификация, установление связей, геолокационная проверка, выявление финансовых следов, мониторинг, подтверждение времени и источника публикации, передача данных, удаленный доступ, профилактические объявления и т.д. Тем самым еще одним основанием классификации может выступать функциональное назначение в расследовании. По этому критерию следует выделить следующие группы ресурсов по ведущей следственной функции:

— поисково-навигационные (поиск по изображениям/видео, по архивам, по форумам);

— идентификационно-атрибутивные (установление принадлежности домена/сайта, привязка аккаунтов, сопоставление псевдонимов, выявление контактных связей);

— коммуникационные (переписка, телеконференции, каналы, чаты, e-mail), включая сведения об электронных сообщениях и сопутствующие метаданные;

— транзакционно-финансовые (платежные интерфейсы, электронные кошельки, личные кабинеты, страницы заказов/оплат, при необходимости —

блокчейн-обозреватели и сервисы анализа транзакций как инструмент реконструкции цепочек);

— геоинформационные и мультимедийные (карты, панорамы, геотеги, фото- и видеохостинги, позволяющие проверять пространственно-временные элементы версии);

— мониторингово-аналитические (системы мониторинга контента, фиксации изменений страниц, выявления повторяющихся публикаций и др.);

— профилактические (доски объявлений, оповещение населения, публикации в СМИ).

Полагаем, что приведенная классификация и описание интернет-ресурсов дадут достаточное представление об их разнообразии и позволят правоприменителю смоделировать с учетом данной видовой классификации постановку и решение типовых задач при расследовании отдельных видов преступлений.

Думается, что включение в предметную область криминалистики закономерностей функционирования цифровых технологий в механизме совершения преступлений, процессов возникновения и отражения следовой информации в сети «Интернет», а также специфики выявления, фиксации, изъятия и использования данных интернет-ресурсов для получения криминалистически значимых сведений о преступной деятельности и ее участниках позволит расширить эмпирическую и, соответственно, основанную на ее познании теоретическую базу ключевых криминалистических учений:

— о криминалистической классификации преступлений за счет выделения дополнительных критериев, позволяющих формировать подвиды частных методик расследования преступлений, совершаемых с использованием ресурсов сети «Интернет». Следует констатировать, что в настоящее время криминалистическая теория находится на этапе активной разработки классификационных критериев для формирования дифференцированных, подвидовых методик расследования преступлений, совершаемых с применением ресурсов сети «Интернет». Необходимость создания особенного научно-методического инструментария для

расследования таких преступлений сегодня признается большинством ведущих представителей криминалистического сообщества[66];

— о механизме преступления путем расширения представлений о закономерностях функционирования цифровых технологий в механизме совершения преступлений. Данное положение в совокупности с видовой классификацией преступлений, совершаемых с использованием сети «Интернет», позволит предложить практическим работникам актуальные рекомендации по моделированию элементов механизма преступления в зависимости от характера интеграции ресурсов Сети в криминальную деятельность. Публикации последних лет подтверждают данное положение. По мнению ряда авторов, ключевая специфика совершения преступлений с использованием сети «Интернет» заключается в том, что данная технология выступает многоаспектным системообразующим элементом способа совершения преступлений. Так, применительно к преступлениям экстремистской направленности ресурсы сети «Интернет» задействуются криминалом одновременно как для публичного распространения радикальных идей, так и для установления и поддержания скрытой коммуникации между членами экстремистских сообществ и организаций[67];

— о личности преступника за счет разработки дополнительных классификационных критериев и типизации лиц, совершающих преступления с использованием ресурсов сети «Интернет». Реализация данного подхода позволит получить углубленную характеристику личности лица, осуществляющего противоправные посягательства посредством сети «Интернет». Кроме того, это даст возможность смоделировать на уровне криминалистической теории закономерные связи между характеристиками личности преступника и иными элементами механизма преступлений различных видов. Например, применительно к дистанционным формам мошенничества, реализуемого посредством сети

---

[66] См., например: Колиев В. В. Тактика и методика расследования преступлений, совершаемых с помощью сети «Интернет» // Право и государство: теория и практика. 2021. № 4 (196). С. 280–282.

[67] См., например: Сайгачева И. А. Методика расследования преступлений экстремистской направленности, совершенных в компьютерных сетях // Контентус. 2025. № 12 (161). С. 14–22.

«Интернет», исследователи указывают на продвинутость современных интернет-мошенников. Такие лица владеют современными компьютерными средствами значительно лучше обычных пользователей, имеют знания и навыки пользования сетью «Интернет» в сфере финансовых услуг. Как правило, это молодые люди в возрасте 20–35 лет. Такой возрастной период обусловлен, как отмечается в литературе, сходством у данных лиц ряда параметров: воспитания, социального статуса, идеологического мышления, уровня восприятия окружающей действительности и т.п.[68] Сформированный таким образом теоретический базис незаменим при разработке эффективных методических и тактико-криминалистических рекомендаций[69];

— о криминалистической ситуалогии посредством типизации ситуаций, возникающих при расследовании преступлений, совершаемых с использованием ресурсов сети «Интернет». Представляется, что криминалистическая ситуалогия не может развиваться имманентно, вне связи с учениями о механизме преступления, личности преступника и пр. Как справедливо отмечается в научной литературе, ситуационные особенности первоначального этапа расследования преступлений, совершенных в сети «Интернет», напрямую детерминированы такими факторами, как объем и характер исходной информации о личности преступника, а также процессуальная форма начальной стадии уголовного судопроизводства[70]. Так, применительно к расследованию мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий[71], к одной из проблем

---

[68] Горбанев В. М., Щербаченко А. К., Бардадым И. С. Личностные характеристики преступников, совершающих мошенничества, связанные с использованием средств сотовой связи // Юристъ-Правоведъ. 2017. № 2. С. 45.

[69] См., например: Родивилин И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 25–29 ; Туркулец В. А., Туркулец И. А., Туркулец С. Е. Типология личности преступника, совершающего преступления против несовершеннолетнего с использованием сети Интернет // Право и практика. 2025. № 1. С. 130–138 и др.

[70] См., например: Виноградова О. П. Типичные следственные ситуации первоначального этапа расследования преступлений, совершаемые с использованием сети Интернет, в отношении несовершеннолетних // Научный вестник ОрЮИ МВД России имени В. В. Лукьянова. 2025. № 1 (102). С. 169–179.

[71] См., например: Сидорова К. С. Алгоритм действий следователя при расследовании мошенничеств, совершаемых дистанционным способом // Закон и право. 2020. № 12. С. 230–233 ; Мазунин Я. М., Сидорова К. С. Следственные ситуации и алгоритм их разрешения при расследовании мошенничеств, совершаемых дистанционным способом в современных условиях // Технологии XXI века в юриспруденции : материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 г.) / под ред. Д. В. Бахтеева. Екатеринбург : Уральский государственный юридический университет, 2020. С. 465–470.

первоначального этапа отдельные авторы вполне обоснованно относят установление места окончания преступного деяния. В результате, как указывается в литературе, складывается ситуация, когда материал предварительной проверки «блуждает» между различными отделами полиции в рамках одного, а чаще разных регионов страны[72];

— о преодолении противодействия расследованию преступлений за счет типизации криминальных приемов, способов и технологий противодействия с использованием современных возможностей устройств доступа к сети «Интернет». При этом развитие данной теории немыслимо без совершенствования вышеперечисленных положений. В частности, следственные ситуации можно классифицировать по степени сведений о преступнике (персонализированных и нет). Например, у следователя на первоначальном этапе могут иметься отдельные сведения о криминальной активности лица в сети «Интернет» (например, диапазон IP, время активности). Однако связать их напрямую с личностью преступника зачастую сложно, поскольку преступник использовал технологии анонимизации (VPN, прокси, TOR), менял географическое положение, маскировал действия;

— о криминалистической профилактике преступлений за счет выявления и устранения причин и условий преступности на основе анализа отражения криминальной активности в сети «Интернет».

Помимо развития частных криминалистических теорий, интеграция в объектно-предметную область криминалистики теоретических положений о возможностях, принципах и направлениях использования сети «Интернет» при решении отдельных тактико-организационных задач расследования позволит конкретизировать практико-ориентированные криминалистические рекомендации по:

— тактике проведения следственных действий с использованием ресурсов сети «Интернет», которая должна в настоящее время строиться на стыке

[72] Лаврушкина А. А. Типичные следственные действия в рамках методики расследования мошенничества с использованием сети Интернет и средств мобильной связи // Бюллетень науки и практики. 2018. Т. 4. № 4. С. 448.

криминалистики, информационных технологий и процессуального права, что подтверждается современными исследованиями в этой области[73];

— системе тактико-организационных рекомендаций по идентификации пользователя в сети «Интернет», базирующейся на поэтапном выявлении совокупности цифровых идентификаторов с последующей верификацией и соотнесением с конкретным физическим лицом;

— системе научно-обоснованных приемов и средств по обнаружению, фиксации и анализу виртуальных следов пользователя на электронных носителях информации. До начала производства следственного действия следователю необходимо четко определить круг криминалистически значимых сведений сетевой активности пользователей (IP-адреса, метаданные файлов, лог-файлы серверов, история авторизаций в аккаунтах, содержимое чатов);

— адаптации методических криминалистических рекомендаций по решению отдельных задач расследования, заключающейся в трансформации классических алгоритмов расследования под специфику интернет-среды;

— обеспечению взаимодействия следственных органов с техническими специалистами и специализированными подразделениями по борьбе с киберпреступностью. В частности, в литературе указывается на возможность привлечения специалистов для анализа лог-файлов, установления принадлежности IP-адресов, выявления следов вредоносного программного обеспечения и восстановления хронологии событий[74];

— оптимизации организации разыскной деятельности за счет использования сведений интернет-ресурсов. В настоящее время единая концепция получения и использования информации из сети «Интернет» в процессе оперативно-разыскной

---

[73] См., например: Ищенко П. П. Следственные действия в условиях цифровизации уголовного судопроизводства // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 30–42 ; Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие. М. : Инфра-М, 2024 ; Тишутина И. В. Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: актуальные вопросы правового обеспечения // Вестник Московского университета МВД России. 2021. № 4 (196). С. 280–282 и др.

[74] См., например: Акиев А. Р., Сотников К. И. Тактика следственного осмотра и исследования цифровой информации средств телекоммуникации и Интернета : учебно-практическое пособие / Санкт-Петербургский университет МВД России. СПб., 2023.

деятельности находится на стадии формирования. Несмотря на концептуальную ясность алгоритмов подобных действий, их правовые основания и тактическая целесообразность во многих случаях остаются дискуссионными[75];

— оптимизации методик экспертных исследований по идентификации лиц, совершающих преступления с использованием ресурсов сети «Интернет».

## § 2. Основные направления поисково-познавательной деятельности следователя по использованию сети «Интернет»

Поисково-познавательная деятельность следователя выступает фундаментальным компонентом расследования и его системообразующим фактором. Она объединяет субъективные качества следователя и объективные элементы следственных ситуаций в единую структуру. Неслучайно в юридической литературе задачи поисково-познавательной деятельности связывают с мысленным реконструированием обстоятельств преступного деяния. Данный процесс реализуется посредством исследования материальных и идеальных носителей криминалистически значимой информации. В дальнейшем эти сведения преобразуются в доказательства с целью установления истины и принятия законных процессуальных решений на стадии возбуждения уголовного дела и предварительного расследования[76].

Анализ юридической литературы позволяет выделить следующие признаки поисково-познавательной деятельности:

— целевой характер. Обусловлен процессуальными и тактико-организационными задачами расследования. Как справедливо отметил И. М. Лузгин, «расследование как познавательный процесс основано на собирании

---

[75] См., например: Шаров В. И. Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. № 2 (64). С. 82–87.

[76] См., например: Корма В. Д., Образцов В. А. К вопросу о структуре и особенностях криминалистической теории следственного познания // Современные проблемы отечественной криминалистики и перспективы ее развития : сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием). Краснодар : Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. С. 60–66.

и переработке следователем информации, под которой понимаются сведения о событии»[77];

— системность. Следует отметить, что достижение высокой результативности при исследовании объектов познания возможно за счет комплексного и взаимосвязанного использования криминалистических средств и методов;

— ситуационность. Данный подход, в сущности, подразумевает рассмотрение различных механизмов развития конкретных следственных ситуаций, знание которых позволяет осуществлять более эффективную криминалистическую подготовку различных субъектов раскрытия и расследования преступлений, в особенности сотрудников следственных подразделений и экспертно-криминалистической службы[78];

— этапность. На первоначальном этапе расследования главным проблемным вопросом является дефицит не только объема криминалистически значимой информации, но и числа ее источников. На протяжении расследования посредством производства следственных действий и оперативно-разыскных мероприятий происходит качественное и количественное расширение информационного массива. С помощью процессуальных действий поступающие сведения проверяются, уточняются, дополняются и преобразуются в доказательства. Всё это позволяет определить ключевые характеристики преступления, в том числе точные данные о месте и времени его совершения. Формируется информационное поле, определяющее мотивы и механизм преступного деяния, конкретизируются сведения об орудиях и о средствах его совершения. На заключительном этапе расследования полученные данные систематизируются и обобщаются, образуя исчерпывающий комплекс знаний о фактах и причинах преступления, что формирует доказательственную базу, которая находит отражение в процессуальных документах;

---

[77] Лузгин И. М. Расследование как процесс познания : дис. ... д-ра юрид. наук. М., 1967. С. 328–334.

[78] Ким В. Д. Следственная ситуация как поисково-познавательная система в криминалистике // Алтайский юридический вестник. 2016. № 3 (15). С. 125–129.

— субъективно-объективный характер. В этой части верно отмечается Р. Л. Ахмедшиным, что поисково-познавательная деятельность характеризуется постоянным поиском, сопровождающимся личным восприятием оперативной обстановки и картины преступления субъектами расследования[79].

Поскольку на процессы собирания, проверки и оценки информации влияют профессиональный опыт и индивидуально-психологические качества следователя, специфика данной деятельности предопределяет предъявление к ее субъекту повышенных требований. В частности, особенности работы с электронными носителями информации обусловливают необходимость привлечения специалиста в соответствии со ст. 164.1 УПК РФ[80]. В связи с этим в юридической литературе справедливо отмечается, что объем процессуальных полномочий и профессиональных компетенций следователя должен коррелировать с характером и уровнем сложности расследуемого уголовного дела[81]. Кроме того, современная цифровизация источников юридически значимых данных повышает риски ошибок при работе с ними. Это обусловливает необходимость непрерывного повышения квалификации следователей с целью формирования устойчивых навыков работы с цифровой информацией[82].

Основываясь на изложенном, мы пришли к выводу, что с криминалистической точки зрения под поисково-познавательной деятельностью следователя понимается система целенаправленных действий по собиранию, исследованию, оценке и использованию доказательственной или иной криминалистически значимой информации в целях раскрытия, расследования и предупреждения преступлений[83].

---

[79] См., например: Ахмедшин Р. Л. Поисковые следственные действия в системе следственных действий: криминалистический аспект // Вестник Томского государственного университета. 2015. № 399. С. 160–166.

[80] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

[81] См., например: Литвинова М. А. Особенности субъективной регуляции деятельности следователя в зависимости от ее сложности // Вестник Самарского юридического института. 2020. № 3. С. 117–126.

[82] См., например: Красненко Ю. В. Поисково-познавательная деятельность на первоначальном этапе расследования // Вестник Белгородского юридического института МВД России. 2019. № 3. С. 52–57.

[83] См., например: Бабакова М. А., Степанов В. В. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий : монография. М. : Юрлитинформ, 2014 ; Криминалистика : учебник для юридических вузов / под ред. В. А. Образцова. М. : Юристъ, 1997 и др.

С учетом того, что в современных реалиях поисково-познавательная деятельность следователя всё чаще смещается в пространство сети «Интернет», возникает необходимость теоретического осмысления ее новых аспектов. В связи с этим целесообразно выделить специфические признаки, присущие поисково-познавательной деятельности в сети «Интернет»:

— виртуализацию следовой картины. Поисково-познавательная деятельность в сети «Интернет» ориентирована на обнаружение виртуальных следов жизнедеятельности лиц или сведений об иных объектах, а также на установление аппаратно-программных средств их создания и обработки. Это обусловливает необходимость исследования виртуальных следов наряду с традиционными материальными и идеальными. В связи с этим В. Б. Вехов, Б. П. Смагоринский и С. А. Ковалев справедливо указывают, что в качестве базовых следообразующих и следовоспринимающих элементов в данном контексте выступают сайт, страница сайта[84];

— экстерриториальность и непрерывность информационного пространства. Ввиду многообразия интернет-ресурсов и возможности удаленного доступа к ним фактически нивелируются пространственно-временные рамки познания. Для следователя это прежде всего означает отсутствие территориальных барьеров при поиске криминалистически значимой информации, а также круглосуточный доступ к источникам данных, устраняющий временны́е ограничения проведения поисковых мероприятий.

Впрочем, с учетом развития и активного использования сети «Интернет» данная деятельность может претерпевать существенные изменения в подходе к ее организации и трансформироваться с учетом применения новых средств и методов[85].

---

[84] Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2. С. 10–19.

[85] См., например: Анешева А. Т., Сидорова К. С. К вопросу о возможностях использования информационно-телекоммуникационной сети «Интернет» в организации раскрытия и расследования преступлений // Пенитенциарная система и общество: опыт взаимодействия : сборник материалов V Международной научно-практической конференции, Пермь, 4–6 апреля 2018 г. / сост. В. А. Овченков. Пермь : ФКОУ ВО Пермский институт ФСИН России, 2018. С. 206–208.

В контексте деятельностного подхода организация процесса по выявлению тактико-организационных особенностей использования ресурсов сети «Интернет» должна детерминироваться осознанной целью. Целеполагание выступает главным критерием содержания и развития данной деятельности, позволяя определить направления использования ресурсов сети «Интернет» при расследовании различных категорий преступлений и производстве следственных действий. В общем виде цель определяется как предвосхищаемый в сознании результат деятельности.

Достаточно четкое определение цели в уголовном судопроизводстве предложено А. Б. Судницыным, который на основе анализа широкого спектра научных точек зрения на эту проблему трактовал цель уголовного судопроизводства как создание условий для реализации уголовной ответственности либо освобождения невиновного от таковой при наличии уголовно-правовых оснований[86]. Рассуждая о цели предварительного расследования, автор говорит о предварительной правовой оценке обстоятельств деяния, обладающего признаками преступления, поскольку устанавливаемые фактические данные создают условия как для досудебного, так и для судебного решения. «Данная правовая оценка основывается на выводах, к которым приходит лицо, ведущее расследование уголовного дела. Возможными вариантами при этом будут либо направление материалов уголовного дела с подготовленными доказательствами в суд, либо прекращение разбирательства по уголовному делу. Непосредственным же содержанием деятельности, направленной на осуществление отмеченной цели, является установление обстоятельств совершенного преступления с последующим принятием процессуального решения»[87].

Соответственно, ресурсы сети «Интернет» при расследовании преступлений также должны использоваться и с целью предварительной правовой оценки

---

[86] См.: Судницын А. Б. Задачи предварительного расследования: правовая природа, система, проблемы реализации и пути совершенствования : монография. Красноярск : СибЮИ МВД России, 2019. С. 42.

[87] Судницын А. Б. Задачи предварительного расследования: правовая природа, система, проблемы реализации и пути совершенствования. С. 52.

обстоятельств посягательства. Для достижения этой цели необходимо установить, в том числе с помощью интернет-ресурсов, обстоятельства совершенного преступления. Однако при установлении этих обстоятельств на пути следователя возникает множество препятствий, которые необходимо преодолеть. Из этих преград рождаются задачи деятельности, четкая постановка и эффективное решение которых позволяют достичь заявленной цели.

Например, А. Б. Судницын предлагает развернутую характеристику задач предварительного расследования, разделяя их на две относительно самостоятельные группы:

— обеспечивающие предварительную правовую оценку деяния, обладающего признаками преступления (своевременное, всестороннее, полное и объективное исследование преступления; изобличение лиц, совершивших преступление, с формулированием и выдвижением обоснованного обвинения; создание предпосылок для участия подозреваемого (обвиняемого) в судебном разбирательстве и надлежащего его поведения при производстве по уголовному делу);

— обеспечивающие защиту прав и законных интересов участников уголовного судопроизводства и профилактику преступлений в досудебном производстве (обеспечение реализации прав участников уголовного судопроизводства и исполнения ими обязанностей; возмещения вреда, причиненного преступлением, других имущественных взысканий, конфискации имущества; безопасности потерпевших, свидетелей и иных участников уголовного судопроизводства, а также их близких; выявление обстоятельств, способствовавших совершению преступления, с правом внесения представления для их устранения; содействие привитию уважительного отношения к законам и неуклонного их исполнения гражданами)[88].

Перечисленные задачи предварительного расследования выводятся из нормативных установлений, которые предписано обязательно выполнять

[88] Судницын А. Б. Задачи предварительного расследования : автореф. дис. ... канд. юрид. наук. Омск, 2009. С. 8.

следователю по каждому уголовному делу. С криминалистических позиций деятельность следователя связана с выбором определенных наиболее эффективных и, главное, целесообразных способов действий. Соответственно, его действия должны предусматривать возможность гибко реализовать тактический замысел и достичь целей расследования в пределах, допустимых законом и полномочиями. Тем самым задачи процессуальные дополняются задачами тактическими, а точнее, трансформируются в них. Г. Л. Грановский, указывая на процессуальные границы решения задачи, трактовал ее как «некоторый объект криминалистической деятельности, направленный на преобразование (с соблюдением процессуальных условий) потенциальной информации, содержащейся в исходных данных (материалах дела) в актуальную доказательную информацию, которая может быть использована для правильного разрешения уголовного дела»[89].

В то же время в криминалистической литературе приводятся определения тактической задачи, которые содержат признаки, не связанные с процессуальной природой ее возникновения и разрешения. Так, В. Е. Корноухов трактует тактическую задачу как часть процесса расследования, отражающую отношение между ситуацией расследования и тактической целью, обусловливающую способ действия[90].

В работе Ю. В. Гаврилина, А. Ю. Головина, И. В. Тишутиной тактическая задача определяется как обусловленная ситуационным фактором необходимость использования сложившихся или создания благоприятных для дальнейшего расследования условий криминалистической деятельности путем оказания тактического воздействия на тот или иной объект[91].

С. Ю. Якушин под тактической задачей понимает «определенную совокупность конкретных вопросов тактического характера, необходимость

---

[89] Грановский Г. Л. Понятие и основные положения теории решения криминалистических задач // Современное состояние и перспективы развития традиционных методов криминалистических экспертиз : сборник научных трудов. М. : Юрид. лит., 1987. С. 5.

[90] См.: Курс криминалистики. Общая часть / отв. ред. В. Е. Корноухов. М., 2000. С. 244.

[91] См.: Гаврилин Ю. В., Головин А. Ю., Тишутина И. В. Криминалистика в понятиях и терминах. М. : Книжн. мир, 2006. С. 115, 117–118.

решения которых вытекает из возникшей следственной ситуации в целях эффективного расследования преступлений»[92].

С точки зрения В. М. Шевчука, тактическая задача — это «ситуационно обусловленная, избирательная, промежуточная цель расследования, достижение которой связано с разрешением с помощью тактических средств ограниченного круга вопросов тактического характера»[93].

В перечисленных работах и трудах других ученых предлагаются классификации тактических задач. Процитируем их по работе В. А. Завьялова, обобщившего их применительно к исследованию проблемы тактических операций:

— по назначению и содержанию: управленческие, розыскные, познавательные, технические;

— по субъекту выдвижения: стоящие перед следователем, выдвинутые специалистами, поставленные в результате коллективной работы субъектов;

— по месту в доказывании: исходные, промежуточные и конечные;

— по приоритетности решения: неотложные и последующие;

— по содержанию: необходимые для изменения сформировавшейся следственной ситуации, для использования следственной ситуации;

— по способам решения возникших задач: простые, сложные;

— по содержанию назначения: познавательные (установление значимых обстоятельств для расследования уголовного дела), управленческие (установление более эффективного взаимодействия с участниками уголовного судопроизводства), организационно-технические (обеспечивающие наиболее эффективный выбор организационно-технических средств).

С точки зрения уровня решаемые тактические задачи подразделяются на исходные (подразумевающие обнаружение, фиксацию и изъятие значимой информации), промежуточные (направленные на получение промежуточных

---

[92] Якушин С. Ю. Тактические задачи при расследовании преступлений: понятие и виды // Ученые записки Казанского государственного университета. Гуманитарные науки. 2010. Т. 152. Кн. 4. С. 207.

[93] Шевчук В. М. Тактические задачи и формирование тактических операций в досудебном производстве [Электронный ресурс] // Электронный журнал «Вестник МГОУ». 2013. № 1. URL: https://www.evestnik-mgou.ru/jour/article/view/843/840 (дата обращения: 11.08.2024).

фактов или формирование тактических комплексов), конечные (при решении которых принимаются тактические и процессуальные решения, а также устанавливаются обстоятельства, входящие в предмет доказывания)[94].

Впрочем, все приведенные дефиниции и классификации не раскрывают в достаточной мере обеспечительный характер тактических задач. Выделение такого количества оснований и дробление по ним задач расследования, на наш взгляд, не несет той практической значимости, которая удовлетворяла бы конкретного правоприменителя.

Анализ выделенных признаков тактической задачи позволил прийти к выводу, что у всех приведенных определений относительно схожая трехчленная структура. Обязательно выделяются:

1) ситуационный фактор, определяемый исходной информацией;

2) требование изменения этого фактора конкретным тактическим способом воздействия;

3) направленность на достижение цели расследования.

Ситуационный фактор является одним из главных, поскольку определяет природу происхождения задачи и ее содержание, а направленность на достижение цели расследования указывает на уголовно-процессуальную обусловленность при ее постановке. С криминалистических позиций шире процессуальных рамок будет объем решаемых вопросов в рамках поставленной тактической задачи.

Обобщая представленные в литературе взгляды на задачи следственной деятельности, можно сделать вывод, что их классификация строится в зависимости от уголовно-процессуальных задач предварительного расследования, а также обусловленного ситуацией расследования содержания и объема. Исходя из этого, можно выделить следующие тактические задачи расследования преступлений по содержательному критерию:

---

[94] См.: Завьялов В. А. Формирование и реализация тактических операций : дис. … канд. юрид. наук. Краснодар, 2021. С. 63–64.

1) раскрытие преступления, под которым понимается установление информации о посягательстве, позволяющей квалифицировать его как преступление, и совершившем его лице;

2) установление лица, потерпевшего от преступления, в том числе личности трупа;

3) задержание лица, совершившего преступление;

4) проверку алиби лиц, возможно причастных к преступлению;

5) изобличение лица, совершившего преступление;

6) розыск обвиняемого, иных лиц, предметов и документов, имеющих значение для дела;

7) выявление и пресечение противодействия расследованию;

8) обеспечение безопасности участников расследования;

9) обеспечение возмещения причиненного преступлением вреда, имущественных взысканий и конфискации;

10) выявление и устранение причин и условий, способствовавших совершению преступления.

Решение перечисленных задач реализуется следователем при расследовании подавляющего большинства преступлений и составляет содержание методик расследования отдельных видов преступлений. В контексте последних универсальный характер обозначенных задач расследования практически любой категории преступлений позволяет разрабатывать общие алгоритмы (программы) для их решения. Однако наличие таких общих алгоритмов не служит осуществлению на практике частных задач расследования. Кроме того, для решения таких задач порой необходимо прибегать к упорядочиванию имеющейся в распоряжении следователя совокупности следственных действий, организационно-технических и других средств согласно единому замыслу, учитывающему отдельные цели расследования и приоритетные направления их достижения. Данная задача реализуется криминалистической наукой в рамках учения о тактических операциях. Последние как раз и наполняют организационную сторону деятельности следователя криминалистически значимой информацией и

конкретными действиями по ее получению, закреплению и использованию относительно следственных ситуаций, этапов расследования, обстоятельств, подлежащих установлению и доказыванию, и пр.

Так, В. М. Шевчук утверждает, что тактические задачи, обусловленные следственными ситуациями, влияют на формирование тактических операций и определяют их содержание[95].

Большинство ученых приходили к выводу о возможности разработки универсальных тактических операций (комбинаций) и их последующей адаптации к расследованию различных видов и групп посягательств. В этой связи особо интересна позиция В. Е. Корноухова, который рассматривал весь процесс расследования как систему тактических задач и операций, что позволяет наиболее полно отразить динамику расследования[96].

Соответственно, целесообразно вести речь об использовании ресурсов сети «Интернет» для обеспечения реализации тактических операций (комбинаций), выделяемых по кругу обозначенных задач.

В процессе расследования следователь стремится к своевременному, полному и объективному установлению обстоятельств преступного деяния путем производства следственных и иных процессуальных действий, а также посредством взаимодействия с органами, осуществляющими оперативно-разыскную деятельность, для реализации оперативно-разыскных мероприятий. Данный вектор не задает императивной программы действий: цель лишь опосредованно влияет на ее формирование, определяя выбор способов достижения результата через решение конкретных тактических задач.

Способом такого достижения будут выступать направленные на решение выделенных задач тактические операции (комбинации), содержание которых необходимо наполнить криминалистически значимой информацией из ресурсов

---

[95] См.: Шевчук В. М. Роль факторов-детерминантов формирования тактических операций при расследовании преступлений // Психопедагогика в правоохранительных органах. 2013. № 2 (53). С. 35.

[96] См.: Корноухов В. Е. О системах тактических задач и операций при расследовании убийств и их специфике на начальном этапе расследования // Проблемы оптимизации первоначального этапа расследования преступлений : межвузовский сборник научных трудов / отв. ред. И. Ф. Герасимов, Л. Я. Драпкин. Свердловск : Свердл. юрид. институт, 1988. С. 85–90.

сети «Интернет» и конкретными действиями по ее получению, закреплению и использованию посредством Сети.

Анализ литературы по данному вопросу позволил классифицировать научные подходы к направлениям использования сети «Интернет» в процессе формирования криминалистических рекомендаций по расследованию преступлений.

1. Узкофункциональный подход. Здесь ученые ограничивают использование сети «Интернет» решением одной конкретной задачи, как правило, вытекающей из результатов изучения определенной видовой разновидности механизма преступления.

Например, из научного труда Т. Ю. Мысливцевой следует вывод о том, что при расследовании преступлений в сфере незаконного оборота наркотических средств и психотропных веществ использование ресурсов сети «Интернет» наиболее значимо для формирования рекомендаций, направленных на получение криминалистической информации о приемах и технологиях коммуникации субъектов, а также о способах подготовки, совершения и сокрытия преступления данного вида, в том числе о технологиях финансовых транзакций и следах, которые свидетельствуют о данных действиях[97].

А. В. Потапов, также исследуя механизм совершения незаконного оборота наркотических средств и психотропных веществ с использованием возможностей сети «Интернет», предложил следующие направления использования Сети для получения криминалистически значимой информации о механизме преступления и лицах, его совершающих: нужно получить информацию об используемых интернет-ресурсах, социальных сетях, через которые осуществляется общение с непосредственными покупателями наркотиков, т.е. установить сайты, аккаунты, через которые идет распространение наркотиков; получив данные об

[97] См.: Мысливцева Т. Ю. Тактические рекомендации при допросах по уголовным делам, связанным с незаконным оборотом наркотических средств, совершенным с использованием сети Интернет // Российский следователь. 2023. № 2. С. 2–6 ; см. также: Анешева А. Т., Сидорова К. С. Проверка сообщения о совершении преступления, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ // Сборник материалов криминалистических чтений. 2017. № 14. С. 6–8.

используемых сайтах, аккаунтах, необходимо попытаться определить виды и место нахождения используемых преступниками средств передачи информации, их IP-адреса; установить используемые для продажи наркотических средств электронные платежные системы, номера счетов, банковских карт с целью получения данных о движении денежных средств по счетам и их использовании преступниками; обладая данными о коде почтового отправления, полученными с использованием специального информационного ресурса, можно отследить перемещения почтовых отправлений, в которых имеются наркотические средства[98].

По сути, ученый ведет речь только о решении одной задачи — получении криминалистически значимой информации о механизме преступления и совершающих его лицах.

2. Многоцелевые подходы. Ученые предлагают выйти за рамки конкретных задач, круг которых определен предметом доказывания по конкретному виду уголовно-наказуемого деяния, и использовать сеть «Интернет» расширительно — для решения сопутствующих криминалистических задач.

В частности, речь идет о следующих векторах применения сети «Интернет» при расследовании преступлений:

— решение тактико-разыскных задач. Так, П. Г. Смагин, С. В. Лемайкина и А. Г. Карпика предлагают расширить использование сети «Интернет» при расследовании преступлений за счет задействования ее возможностей в процессе розыска лиц; оповещения населения о преступлениях и преступниках; установления стоимости похищенного[99]. В этом случае расширяется круг тактических задач расследования за счет внедрения сети «Интернет» в разыскную деятельность;

---

[98] Потапов А. В. Возможности применения сети Интернет в расследовании преступлений: тактические и правовые аспекты // NovaInfo.Ru. 2017. Т. 4. № 58. С. 363–367.

[99] Смагин П. Г., Лемайкина С. В., Карпика А. Г. Использование информационных сервисов сети Интернет при расследовании преступлений // Актуальные проблемы теории и практики уголовного процесса : сборник материалов Международной научно-практической конференции. Ростов н/Д. : Ростовский юридический институт МВД России, 2018. С. 35–41.

— решение технологических/инструментальных задач расследования. Например, А. А. Аубакирова заострила внимание научной общественности и практиков на отдельных направлениях использования сети «Интернет» при проведении следственных действий, в частности при проведении предъявления для опознания в онлайн-режиме[100]. В данном случае автор подчеркивает модернизацию формы проведения конкретных следственных действий путем их переноса в онлайн-пространство;

— решение организационных задач расследования, в частности проведение онлайн-совещаний по сложным делам в целях повышения оперативности решения отдельных задач расследования;

— обеспечение версионной деятельности посредством свободного доступа к информационным базам. Речь идет о внедрении в практику расследования ресурсов открытого доступа — OSINT. К таким ресурсам относятся сайты и страницы, доступные без специальных прав (публичные профили, открытые каналы, реестры, публикации организаций, открытые базы судебных актов и т.п.). Информация из этих ресурсов извлекается без преодоления технических средств защиты и без обращения к закрытым учетным данным. При этом даже открытость не снимает требований к корректной фиксации, поскольку контент динамичен и легко модифицируется или удаляется. Поэтому при выявлении значимой информации ключевым становится своевременное документирование факта ее существования. Полученные из таких источников сведения позволяют объективизировать версионную деятельность по многим важным направлениям расследования, в частности составлению субъективного портрета преступника, его психологического профиля или определению возможного круга общения или мест пребывания и пр.

[100] Аубакирова А. А. Возможности использования Интернета при расследовании и профилактике преступлений // Информатизация и информационная безопасность правоохранительных органов. М. : Академия управления МВД России, 2008. С. 338–343.

3. Обеспечительные подходы. Сеть «Интернет» рассматривается преимущественно как внешняя информационно-телекоммуникационная инфраструктура, направленная на:

— решение задач, связанных с электронным документооборотом и консультированием. В. Б. Вехов выделяет в качестве вспомогательных следующие направления использования сети «Интернет» в расследовании преступлений: получение консультационной правовой помощи, правовых и нормативных документов, а также генерацию бланков процессуальных документов с помощью информационных ресурсов Сети — веб-сайтов Государственной Думы, Совета Федерации, Президента, Правительства, Верховного Суда и других органов государственной власти Российской Федерации, — а также с помощью автоматизированных справочно-правовых систем «Гарант», «КонсультантПлюс», «Кодекс» и пр.; служебную переписку по находящимся в производстве уголовным делам, получение директивных, справочно-нормативных документов и методических материалов[101];

— решение информационных задач в процессе принятия тактических и процессуальных решений. А. И. Гайдин представил ви́дение направлений использования ресурсов сети «Интернет» в деятельности органов предварительного расследования как источников информации, непосредственно не связанных с событием преступления, но имеющих значение для установления отдельных обстоятельств дела, принятия организационно-тактических и процессуальных решений (справочная информация, персональная информация отдельных лиц, сведения об учреждениях и организациях, описания внешнего вида и технических характеристик объектов, фигурирующих в расследовании, и другие материалы); в качестве оперативного источника получения доступа к постоянно пополняющимся базам данных законодательных актов, научной и методической

[101] Подробно см.: Цифровая криминалистика : учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024.

информации, а также судебной практики по уголовным делам всех регионов России[102].

4. Системно-деятельностный (комплексный) подход. Данный подход объединяет различные взгляды ученых в единую систему. Мы также придерживаемся данного подхода и считаем, что в процессе расследования преступлений реализуются преимущественно следующие два направления использования сети «Интернет»:

1) в качестве цифровой технологии поиска и анализа поисковых признаков объектов розыска: людей, трупов и их частей, животных, вещественных доказательств, транспортных средств, имущества и пр.;

2) в качестве цифровой технологии собирания криминалистически значимой информации для установления обстоятельств, подлежащих доказыванию по уголовному делу, где основное внимание уделяется ее использованию для поиска, фиксации, изъятия и анализа доказательств, размещенных на ее ресурсах, при производстве следственных действий (осмотр места происшествия, допрос, предъявление для опознания, обыск, выемка и пр.)[103].

Проведенный анализ теоретических позиций наглядно демонстрирует эволюцию научной мысли: от узкофункционального восприятия сети «Интернет» как локального источника сведений по конкретным составам преступлений и вспомогательного справочного информационно-обеспечительного инструмента к многоцелевым тактическим моделям. Данная тенденция логически завершается переходом к системно-деятельностному подходу, рассматривающему сеть «Интернет» как динамично развивающуюся среду, в рамках которой решаются комплексно следственные, разыскные и обеспечительные задачи расследования.

---

[102] Гайдин А. И. Использование информационных ресурсов Интернет в расследовании преступлений // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : материалы Всероссийской научно-практической конференции. Орел : Орловский юридический институт имени В. В. Лукьянова, 2016. С. 89–90.

[103] См.: Сидорова К. С. Направления поисковых действий следователя в информационно-телекоммуникационной сети «Интернет» при расследовании преступлений // Актуальные проблемы расследования преступлений : материалы Всероссийской научной конференции памяти И. Ф. Герасимова (Екатеринбург, 31 января 2020 года) / под ред. Д. В. Бахтеева. Екатеринбург : Уральский государственный юридический университет, 2020. С. 135–143.

Тем не менее с учетом обобщения данных проведенного ранее исследования и приведенных точек зрения мы пришли к выводу: разделение ресурсов сети «Интернет» на источник информации и средство ее получения позволяет конкретизировать организационные формы использования этих ресурсов в расследовании преступлений. При этом их выбор обусловливается задачами по обнаружению, фиксации, изъятию, исследованию и использованию криминалистически значимой информации, решаемыми посредством тактических комбинаций и операций.

Выделение видов криминалистических операций по содержанию решаемых задач имеет место в работах многих ученых-криминалистов. Так, В. И. Шиканов в классификации по основанию цели, которую предполагается достичь в результате осуществления тактической операции, отграничивал розыск, проверку, разоблачение, установление обстоятельств, способствующих преступлению, и т.д.[104]

В классификации В. А. Образцова по содержанию задач операции группируются в обеспечивающие поиск людей и обнаружение предметов[105]. Н. Ю. Пономаренко выделяет такие операции, как «собирание косвенных доказательств, обеспечение следственной тайны, изобличение обвиняемого, установление потерпевшего, установление обстоятельств, способствующих преступлению, предвосхищающая проверка алиби подозреваемого, обвиняемого, проверка и объективизация признательных показаний подозреваемого, обвиняемого, показаний других лиц, реконструкция отдельных обстоятельств преступления, досудебное соглашение о сотрудничестве»[106].

Между тем не все из выделенных по содержанию задач операций могут представлять, на наш взгляд, отдельный самостоятельный тактический комплекс действий. Такая задача, как изучение личности подозреваемого (обвиняемого),

---

[104] Шиканов В. И. Актуальные вопросы уголовного судопроизводства и криминалистики в условиях современного научно-технического прогресса: на материале процессуальных и криминалистических исследований уголовных дел об убийстве. Иркутск : Изд-во Иркутского ун-та, 1978. С. 147–148.

[105] Подробно см.: Образцов В. А. Выявление и изобличение преступника. М. : Юристъ, 1997.

[106] Понятие, классификация и структура тактических операций в расследовании преступлений : научно-практическое пособие / под ред. Н. Ю. Пономаренко. Белгород, 2017. С. 36–37.

может быть разрешена в рамках других тактических операций (розыск скрывшегося обвиняемого, задержание подозреваемого, изобличение лица, совершившего преступление, и пр.). Объем решения этой задачи и обеспечивающий характер по отношению к другим операциям требуют определения самостоятельного комплекса действий. Кроме того, уголовно-процессуальная норма диктует отдельное решение этой задачи, определяя в п. 3 ч. 1 ст. 73 УПК РФ необходимость установления и доказывания обстоятельств, характеризующих личность обвиняемого.

Анализ приведенных взглядов на сущность тактической операции позволяет сделать выводы о ключевых признаках, которым должна отвечать тактическая операция по использованию ресурсов сети «Интернет» при расследовании преступлений.

1. Комплексность и программность составляющих тактической операции: операция не сводится к единичному поиску в сети «Интернет», она включает несколько согласованных действий, реализуемых в логической последовательности (например, «осмотр интернет-страницы → выемка устройства → запрос сведений у организатора распространения информации в сети “Интернет” (провайдера) → назначение экспертизы»).

2. Единый замысел и ситуационная корреляция: операция строится вокруг конкретной задачи (установить лицо, проверить версию, выявить канал сбыта, обеспечить сохранность данных, найти свидетелей и т.п.) и ситуации (например, начальная стадия подготовки преступления может проходить на одном интернет-ресурсе, а последующие переговоры — на другом, что затрудняет отслеживание действий правоохранительными органами, поскольку каждая отдельная переписка выглядит изолированной и не связанной с остальными).

3. Направленность на получение сведений, имеющих поисково-ориентирующее и доказательственное значение: итогом операции должны становиться не только ориентирующие сведения (мониторинг интернет-пространства (например, чатов) в целях поиска преступника и сбора ориентирующих данных о нем), но и результаты, которые могут быть проверены и

использованы в доказывании при соблюдении процессуальных требований (в том числе к работе с электронными носителями и копированию информации).

4. Учет тактики риска в условиях динамичности данных: интернет-контент изменяем и легко удаляется, что требует тактических решений по срочной фиксации, сохранению и верификации сведений. Например, преступники применяют специализированные программы, или скрипты (так называемые макросы), предназначенные для автоматического уничтожения следов их присутствия на интернет-ресурсе либо на конкретном устройстве. Эти макросы способны стереть журналы посещений веб-сайтов, файлы cookie, кэш браузера и прочие следы цифровой активности, тем самым предотвращая обнаружение пользователями и правоохранительными органами. Поэтому при организации тактической операции по проникновению в кол-центр надо предусмотреть, что криминалистически значимые сведения могут быть удалены, поэтому решается вопрос о привлечении дополнительных специалистов.

5. Техническая готовность: при проведении тактической операции могут понадобиться технические средства для обнаружения, фиксации[107] и изъятия криминалистически значимой информации, которые необходимо подготовить заблаговременно.

6. Сочетание следственных действий, оперативно-разыскных и организационно-технических мероприятий. Проведенное обобщение материалов уголовных дел позволило сделать вывод, что задействование ресурсов сети «Интернет» в рамках большинства решаемых задач расследования может быть реализовано в двух организационных формах: как источник криминалистически значимой информации (63 % изученных уголовных дел) и как средство выявления, фиксации и передачи криминалистически значимой информации (44 % изученных уголовных дел).

---

[107] См., например: Сидорова К. С. Способы фиксации информации, полученной с использованием ресурсов сети Интернет // Преемственность и новации в юридической науке : материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей, Омск, 21 мая 2019 г. Омск : Омская академия Министерства внутренних дел РФ, 2019. С. 95–97.

7. Ситуационная обусловленность. Применение тактических приемов, тактических комбинаций и операций на практике предопределено конкретными ситуациями расследования. Они являются основными средствами воздействия на данные ситуации в целях принятия процессуальных и тактических решений.

На наш взгляд, под тактической операцией по использованию ресурсов сети «Интернет» в расследовании преступлений следует понимать комплексное криминалистическое средство планомерного решения локальных задач расследования, связанных с поиском, фиксацией, проверкой и процессуальным закреплением информации, содержащейся в интернет-ресурсах, хранящейся на программно-аппаратных средствах. Ее специфика обусловливается динамичностью трансформации цифровых объектов, многообразием источников криминалистически значимой информации, рисками утраты данных и ошибок в процессе их интерпретации[108].

Проведенное обобщение следственной практики позволило сделать вывод о следующих ключевых направлениях реализации тактической операции по использованию ресурсов сети «Интернет» при расследовании преступлений:

— установление информации о посягательстве, позволяющей квалифицировать его как преступление, и сведений о совершившем его лице (92 %);

— установление лица, потерпевшего от преступления, в том числе личности трупа (22 %);

— изучение личности лица, совершившего преступление (84 %);

— задержание лица, совершившего преступление (18 %);

— проверка алиби лиц, возможно причастных к преступлению (48 %);

— изобличение лица, совершившего преступление (62 %);

[108] См.: Белова К. С. Тактическая операция по использованию ресурсов сети «Интернет» при расследовании преступлений [Электронный ресурс] // Шикановские криминалистические чтения: криминалистическое и судебно-экспертное обеспечение расследования и раскрытия преступлений : материалы ежегодной Всероссийской научно-практической конференции молодых исследователей, Иркутск, 17 декабря 2025 г. / отв. ред. Д. А. Степаненко. Иркутск : Изд. дом БГУ, 2026. С. 5–9. URL: http://lib-catalog.bgu.ru.

— привлечение подозреваемого (обвиняемого) к сотрудничеству путем заключения досудебного соглашения о сотрудничестве (9 %);

— розыск обвиняемого, иных лиц, предметов и документов, имеющих значение для уголовного дела (76 %);

— выявление и пресечение противодействия расследованию (35 %);

— обеспечение безопасности участников расследования (5 %);

— обеспечение возмещения причиненного преступлением вреда, имущественных взысканий и конфискации (28 %);

— выявление и устранение причин и условий, способствовавших совершению преступления (12 %)[109].

Результаты эмпирического исследования (92 % и 84 % соответственно) подтверждают, что ресурсы сети «Интернет» чаще всего используются для решения базовых тактических задач по установлению особенностей механизма преступления и изучению личности преступника. В то же время практика расследования демонстрирует значительный потенциал использования ресурсов сети «Интернет» на всех этапах досудебного производства — от проверки алиби (48 %) и розыска (76 %) до обеспечения возмещения вреда (28 %) и устранения причин и условий, способствующих совершению преступления (12 %).

Это подтверждает ранее выдвинутый тезис о том, что задачи расследования, реализуемые с использованием сети «Интернет», выходят за пределы только поиска информации. Они охватывают весь спектр криминалистической деятельности, что обусловливает необходимость организации данной работы в форме тактических операций (комбинаций).

Вместе с тем следует обозначить специфику реализации выделенных направлений за счет обращения к интернет-ресурсам. Она будет проявляться в выполнении частных задач использования сети «Интернет», возникающих внутри

---

[109] Относительно решения последней задачи вряд ли потребуется применять операционный метод, но и исключать этого не следует, поскольку комбинация определенных действий и приемов в любом случае будет иметь место.

См. подробно: Белова К. С. Направления использования ресурсов сети «Интернет» при решении задач расследования преступлений // Российский следователь. 2026. № 1. С. 2–6.

каждой операции. Обусловленные общей целью получения криминалистически значимой для расследования конкретного преступления информации, должны быть выделены и решены по каждой операции следующие частные задачи:

1. Информационно-поисковая: выявление сообщений, публикаций, объявлений, фото/видео, цифровых документов, следов транзакций, репостов, резервных копий. Так, в рамках производства по уголовному делу о преступлении против здоровья населения и общественной нравственности посредством проведения автоматизированного осмотра закрытого интернет-ресурса была решена задача — выявление факта совершения данного вида преступления. В частности, как было установлено, в целях незаконного сбыта наркотиков лицо разместило в сети «Интернет» сообщения о местонахождении наркотических средств в виде рекламы с предложением приобрести их через сеть «Интернет»[110].

2. Идентификационная: сопоставление инфраструктуры с данными о конкретном лице (установление личности, зарегистрированной под аккаунтом / ником / номером телефона; сопоставление цифровых идентификаторов (электронная почта, номера, устройства, IP-адрес) с конкретным лицом). Так, в приговоре Ленинского районного суда г. Иваново в качестве доказательств, подтверждающих вину подсудимого, исследован ответ на запрос в АО «Киви Банк». К ответу был приложен CD-диск с файлом .xls, в котором содержалась таблица с информацией об аккаунте подсудимого. В ней были указаны дата создания кошелька, дата последнего входа, IP-адрес последнего входа и имя владельца электронного кошелька[111].

3. Версионно-проверочная: проверка следственных версий и алиби через виртуальные хронологии, геолокационные следы, время активностей, подтверждение/опровержение контактов. Согласно приговору Ханты-Мансийского районного суда Ханты-Мансийского автономного округа — Югры с

---

[110] См., например: приговор Новочебоксарского городского суда Чувашской Республики от 27.11.2025 по делу № 1-314/2025 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/3yI8tO5rr6Nv/ (дата обращения: 22.06.2026).

[111] Кулаевский А. В. Виды следов, способствующих установлению лица, совершившего дистанционное мошенничество // Matters of Russian and International Law. 2024. Vol. 14. Is. 7A. P. 452.

целью проверки алиби и показаний подсудимых с помощью информации, предоставленной мобильным оператором ООО «Т2 Мобайл», было установлено, что мобильный телефон находился в зоне действия базовой станции вблизи места совершения преступления[112].

4. Доказательственная: процессуальное закрепление и обеспечение воспроизводимости информации (протоколирование, участие специалиста, контроль целостности, назначение экспертиз). В судебной практике (например, в решениях по делам о преступлениях в сфере компьютерной информации) данная функция реализуется через строгий алгоритм фиксации: привлечение специалиста в сфере информационных технологий для изъятия электронного носителя информации, вычисление криптографических хеш-функций для контроля неизменности данных и их обязательное занесение в протокол следственного действия, например осмотра. Последующее назначение судебной компьютерной экспертизы и сверка хеш-сумм позволяют верифицировать подлинность информации[113].

5. Обеспечительная: предотвращение утраты данных (удаление аккаунта/контента, исчезающие сообщения, ограниченные сроки хранения логов). Анализ судебной практики показывает: данная функция реализуется через применение различных тактических приемов при проведении следственных действий, например перевод изъятых мобильных телефонов в авиарежим для недопущения дистанционного удаления данных с устройства, немедленная фото- и видеофиксация экранов устройств и т.д.

6. Коммуникативная: выявление свидетелей или потерпевших через ресурсы сети «Интернет» (участники чатов, покупатели на маркетплейсах и т.п.). При анализе материалов уголовных дел было выявлено, что данная функция

---

[112] Приговор Ханты-Мансийского районного суда Ханты-Мансийского автономного округа — Югры от 01.02.2017 № 1-4/2017 1-451/2015 1-53/2016 по делу № 1-4/2017 [Электронный ресурс] // URL: https://sudact.ru/regular/doc/pUINI7jb9aLV/ (дата обращения: 08.07.2026).

[113] См., например: приговор Железнодорожного городского суда Московской области от 04.12.2025 № 1-328/2025 по делу № 1-328/2025 [Электронный ресурс] // URL: https://sudact.ru/regular/doc/C3ewRvSJYB1X/ (дата обращения: 08.07.2026).

реализуется при анализе истории финансовых транзакций, переписок на интернет-ресурсах и т.д.

## Выводы по первой главе

1. Сеть «Интернет» в силу своего содержания и специфического устройства является самостоятельным объектом познания криминалистической науки — элементом функциональной стороны криминальной и антикриминальной деятельности. Это обусловливает необходимость включения в предметную область криминалистики закономерностей не только применения цифровых технологий при подготовке, совершении и сокрытии преступлений, но и возникновения и отражения следов преступления в информационно-телекоммуникационной сети «Интернет», выявления, фиксации, изъятия и использования данных из интернет-ресурсов для получения криминалистически значимых сведений о преступной деятельности и ее участниках.

2. Под используемыми в расследовании информационными ресурсами понимается системно обусловленная, принципиально достижимая, потребляемая и эффективная информация, способствующая установлению наличия или отсутствия обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для дела.

3. Применительно к использованию в уголовном судопроизводстве ресурс сети «Интернет» можно определить как информационную технологию, содержащую системно обусловленную, принципиально достижимую с помощью программно-аппаратных средств, потребляемую информацию, способствующую эффективному решению задач расследования преступлений.

4. Выделены структурные элементы сети «Интернет», содержащие требуемые для расследования ресурсы: электронная почта (e-mail), информационная сеть WWW, электронные доски объявлений BBS, системы телеконференций, система файловых архивов FTP, информационные системы,

информационные ресурсы, каталоги X.500, справочные службы, система TRICKLE, протоколы для удаленного доступа к ресурсам, совокупность различных мессенджеров и социальных сетей, электронные торговые площадки, нейросети.

5. По правовому режиму доступа и способу легитимного получения сведений интернет-ресурсы подразделяются на ресурсы открытого доступа (OSINT-сегмент), условно-открытого доступа, закрытого доступа (ресурсы анонимизированного/скрытого сегмента).

По субъекту владения и управления выделяют государственные и муниципальные ресурсы, коммерческие платформы и сервисы, инфраструктурные субъекты интернет-среды, пользовательские (социальные) ресурсы.

По функциональному назначению в расследовании интернет-ресурсы бывают поисково-навигационными, идентификационно-атрибутивными, коммуникационными, транзакционно-финансовыми, геоинформационными и мультимедийными, мониторингово-аналитическими, профилактическими.

6. Под поисково-познавательной деятельностью следователя понимается система целенаправленных действий по собиранию, исследованию, оценке и использованию доказательственной или иной криминалистически значимой информации в целях раскрытия, расследования и предупреждения преступлений.

7. Выделены следующие тактические задачи расследования преступлений по содержательному критерию:

1) раскрытие преступления, под которым понимается установление информации о посягательстве, позволяющей квалифицировать его как преступление, и совершившем его лице;

2) установление лица, потерпевшего от преступления, в том числе личности трупа;

3) задержание лица, совершившего преступление;

4) проверка алиби лиц, возможно причастных к преступлению;

5) изобличение лица, совершившего преступление;

6) розыск обвиняемого, иных лиц, предметов и документов, имеющих значение для дела;

7) выявление и пресечение противодействия расследованию;

8) обеспечение безопасности участников расследования;

9) обеспечение возмещения причиненного преступлением вреда, имущественных взысканий и конфискации;

10) выявление и устранение причин и условий, способствовавших совершению преступления.

8. Разграничение ресурсов сети «Интернет» на источник информации и средство ее получения позволяет выделить организационные формы использования этих ресурсов в расследовании преступлений, выбор которых обусловливается задачами по обнаружению, фиксации, изъятию, исследованию и использованию криминалистически значимой информации, решаемыми посредством тактических комбинаций и операций. Ресурсы сети «Интернет» во всех выделенных по содержанию решаемых тактических задач криминалистических операциях могут быть реализованы в двух организационных формах: как источник криминалистически значимой информации и как средство выявления, фиксации и передачи криминалистически значимой информации.

9. Под тактической операцией по использованию ресурсов сети «Интернет» в расследовании преступлений следует понимать комплексное криминалистическое средство планомерного решения локальных задач расследования, связанных с поиском, фиксацией, проверкой и процессуальным закреплением информации, содержащейся в интернет-ресурсах, хранящейся на программно-аппаратных средствах. Ее специфика обусловливается динамичностью трансформации цифровых объектов, многообразием источников криминалистически значимой информации, рисками утраты данных и ошибок в процессе их интерпретации.

10. Выделены следующие ключевые направления реализации тактической операции по использованию ресурсов сети «Интернет» при расследовании преступлений:

— установление информации о посягательстве, позволяющей квалифицировать его как преступление, и сведений о совершившем его лице;

— установление лица, потерпевшего от преступления, в том числе личности трупа;

— изучение личности лица, совершившего преступление;

— задержание лица, совершившего преступление;

— проверка алиби лиц, возможно причастных к преступлению;

— изобличение лица, совершившего преступление;

— привлечение подозреваемого (обвиняемого) к сотрудничеству путем заключения досудебного соглашения о сотрудничестве;

— розыск обвиняемого, иных лиц, предметов и документов, имеющих значение для уголовного дела;

— выявление и пресечение противодействия расследованию;

— обеспечение безопасности участников расследования;

— обеспечение возмещения причиненного преступлением вреда, имущественных взысканий и конфискации;

— выявление и устранение причин и условий, способствовавших совершению преступления.

# Глава II. АЛГОРИТМЫ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» В ЦЕЛЯХ ПОЛУЧЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

## § 1. Использование ресурсов сети «Интернет» в установлении информации о событии преступления и совершившем его лице

В предыдущем параграфе в качестве одной из тактических задач мы выделяли раскрытие преступления, под которым понимается установление информации о посягательстве, позволяющей квалифицировать его как преступление, и совершившем его лице. Относительно содержания понятия «раскрытие преступления» ведется длительная научная дискуссия.

Обратимся к словарному толкованию понятия «раскрытие». В словаре С. И. Ожегова, Н. Ю. Шведовой «раскрыть» — значит «обнаружить, сделать известным, объяснить»[114]. В словаре Т. Ф. Ефремовой «раскрывать» означает «обнаруживать, находить, делать известным неизвестное, скрываемое, устанавливать путем исследований, наблюдений»[115].

В юридической литературе распространено мнение, что существует три подхода к определению указанного понятия: уголовно-процессуальный, криминалистический и оперативно-разыскной[116], анализ которых позволяет утверждать: невозможно однозначно разделить существующие точки зрения на указанные отраслевые группы, поскольку как исследователи-криминалисты, так и

---

[114] Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка [Электронный ресурс]. М. : Азъ, 1992. URL: https://www.lib.ru/DIC/OZHEGOW/ozhegow_p_r.txt (дата обращения: 21.02.2024).

[115] Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный [Электронный ресурс]. М. : Русский язык, 2000. URL: https://www.efremova.info/word/raskrytie.html (дата обращения: 21.02.2023).

[116] См.: Вандышев В. А., Робозеров В. Я. Раскрытие преступлений, совершенных в условиях неочевидности. Л., 1990. С. 16 ; Ахмадуллин А. С. Понятия «раскрытие преступления», «выявление преступления», «очевидное и неочевидное преступления», используемые при формировании официальной правовой статистики // Законность. 2017. № 9. Сент. С. 45–48 ; Потапов С. А. Основные аспекты, характеризующие понятие раскрытие преступления // Актуальные проблемы государства и права. 2022. Т. 6. № 1. С. 86–92 ; Айвазова О. В. К вопросу о сущности понятия «раскрытие преступления» в контексте норм действующего законодательства // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 21 ; Низамов В. Ю. К вопросу о понятии «раскрытие преступления» в криминалистике и уголовном процессе // Ленинградский юридический журнал. 2016. № 1 (43). С. 170–179 ; Конин А. В., Ялышев С. А. Раскрытие преступления: субъекты и алгоритм // Криминалист. 2021. № 4 (37). С. 75–80, и пр.

ученые в сфере наук уголовного процесса и оперативно-разыскной деятельности не придерживаются единой, взятой за основу концепции.

На наш взгляд, если и вести речь о группировке подходов к определению понятия раскрытия преступления, то исходя из критерия объема и пределов деятельности (что именно должно быть сделано и в каком объеме) по расследованию и конкретного процессуального решения по уголовному делу (какое юридическое решение должно быть принято). В этом смысле раскрытие является частью процесса расследования.

С этих позиций в юридической литературе выделяются мнения о том, что преступление считается раскрытым, когда:

1) установлены событие преступления и лицо, его совершившее[117];

2) объем установленных данных о преступлении и виновном в его совершении лице позволяет предъявить обвинение[118];

3) полностью установлен предмет доказывания по делу, что дает основание принять решение об окончании расследования[119];

4) виновность конкретного лица установлена приговором суда[120].

Не останавливаясь на анализе аргументов приверженцев каждого подхода, что уже в достаточной мере проведено в научных исследованиях[121], отметим

---

[117] См.: Карпец И. И. Проблема преступности. М., 1969. С. 152 ; Михайлов А. И., Сергеев Л. А. Процессуальная сущность раскрытия преступления // Советское государство и право. 1971. № 4. С. 112 ; Калинин Ю. В. О понятии раскрытия преступлений // Вопросы криминалистической методологии, тактики и методики расследования. М., 1973. С. 35–36 ; Якубович Н. А. Процессуальные функции следователя // Проблемы предварительного следствия в уголовном судопроизводстве : сборник научных трудов. М., 1980. С. 17 и др.

[118] См.: Веселов Ю. И. Понятие полного раскрытия преступлений // Сборник статей адъюнктов и соискателей. Вып. 3. М., 1971. С. 30 ; Гаврилов А. К. Раскрытие преступлений на предварительном следствии (правовые и организационные вопросы). Волгоград, 1976. С. 25 ; Герасимов И. Ф. Некоторые проблемы раскрытия преступлений. Свердловск, 1975. С. 50 ; Лавдаренко Л. И. Раскрытие преступления как одна из задач органов предварительного расследования // Сибирский юридический вестник. 2013. № 1 (60). С. 100 и др.

[119] См.: Жогин Н. В., Фаткуллин Ф. Н. Предварительное следствие в советском уголовном процессе. М., 1965. С. 38 ; Викторов Б. А. Общие условия предварительного расследования. М., 1971. С. 5–7 ; Волов В. Г. Об оценке эффективности деятельности по раскрытию преступлений // Вопросы раскрытия и расследования преступлений : сборник научных трудов. М., 1982. С. 28 и др.

[120] См.: Лузгин И. М. Расследование как процесс познания. М., 1969. С. 16 ; Скоромников К. С. Существующая система учета преступлений и раскрытия их нуждается в кардинальной реформе // Государство и право. 2000. № 1. С. 108 ; Дяблова Ю. Л. Некоторые аспекты соотношения раскрытия и расследования преступлений // Известия Тульского госуниверситета. 2009. № 1. С. 363 ; Чупилкин Ю. Б. Содержание категорий «раскрытие», «расследование» и «раскрываемость» преступлений в российском законодательстве // Российская юстиция. 2019. № 4. С. 35 и др.

[121] См.: Судницын А. Б. Задачи предварительного расследования: правовая природа, система, проблемы реализации и пути совершенствования. С. 77–84 ; Айвазова О. В. Указ. соч. ; Потапов С. А. Указ. соч. и др.

основной выделяемый в любом подходе признак раскрытия — наличие и объем информации о лице, совершившем преступление. Еще в 1970-х гг. Ф. Ю. Бердичевский указал, что содержанием раскрытия преступления выступает деятельность по расследованию, осуществляемая в условиях отсутствия информации, делающей известной личность преступника[122]. А в последующем согласно содержанию законодательных и подзаконных нормативных актов вплоть до принятия УПК РФ представление о раскрытом преступлении однозначно связывалось с обнаружением преступника.

Дискуссию же вызывает объем этой информации, позволяющий прийти к однозначному утверждению о совершении посягательства конкретным человеком.

На наш взгляд, с этих позиций выделенные четыре подхода могут быть представлены следующим образом:

1) обстоятельства преступления указывают на конкретное лицо, но пока не исключают причастность других (на уровне основной версии);

2) с большой вероятностью преступление совершило конкретное лицо, и отсутствуют обстоятельства, указывающие на его непричастность или причастность иных лиц;

3) высший уровень уверенности в совершении преступления конкретным лицом, исключающий какую-либо его непричастность;

4) однозначно доказано, что преступление совершило конкретное лицо, признанное судом преступником (либо уголовное преследование в отношении которого прекращено по нереабилитирующим основаниям).

Таким образом, очевидно, что получение информации о причастности определенного лица к преступлению порождает задачу проверки его алиби, изучения его личности, его изобличения, в случае сокрытия — его розыска, в случае противодействия — нейтрализации такой деятельности и пр. Тем самым, если связывать содержание понятия «раскрытие преступления» с процессуальными моментами предъявления обвинения, окончания расследования

[122] См.: Бердичевский Ф. Ю. О предмете и понятийном аппарате криминалистики // Вопросы борьбы с преступностью. Вып. 24. М., 1976. С. 131–149.

или вынесения приговора, мы приходим к смешению между собой разнородных задач предварительного расследования.

С нашей точки зрения, если раскрытие преступления связывается с установлением сведений о лице, его совершившем, то определяющая задачу категория должна одновременно характеризоваться как получением этой информации и обладанием ею, так и объемом, и пределами ее познания, не вторгающимися в поле возникновения и разрешения других, последующих задач.

Как верно указывал Р. С. Белкин, «раскрытие — это деятельность по расследованию преступления, направленная на получение информации, дающей основание к выдвижению версии о совершении преступления определенным лицом»[123].

С позиции специфики деятельности по расследованию преступлений и ее поисково-познавательного характера в этимологии понятия «раскрытие» первоначальной, определяющей категорией выступает «обнаружение». Перед следователем в первую очередь возникает задача найти, отыскать, обнаружить информацию, указывающую на то, что произошедшее событие содержит признаки преступления. Следовательно, далее необходимо ответить на вопрос, кто его совершил, а также обнаружить, отыскать информацию об определенном человеке и о связи его личности и его действий с противоправным результатом. Однако отыскание и обнаружение информации — это процесс поисково-познавательной деятельности, не всегда предполагающий глубокий анализ полученных сведений. Формулировка же окончательных выводов о событии преступления и причастности лица есть результат аналитических умозаключений. Именно поэтому данный поисково-познавательный процесс целесообразно определять через более широкую категорию «установление», которая означает не просто «обнаружить», но и «определить, выяснить, доказать»[124].

---

[123] Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 3 : Криминалистические средства, приемы и рекомендации. С. 383.

[124] Словарь русского языка : в 4 т. [Электронный ресурс] / РАН, Ин-т лингвистич. исследований ; под ред. А. П. Евгеньевой. 4-е изд., стер. М. : Рус. яз. ; Полиграфресурсы, 1999. URL: https://feb-web.ru/feb/mas/mas-abc/20/ma452404.htm?cmd=0&istext=1 (дата обращения: 21.02.2024).

Таким образом, с позиции классификации задач предварительного расследования обоснованно выделить в качестве первоочередной задачу по установлению фактических данных, позволяющих квалифицировать деяние и идентифицировать лицо, его совершившее. В рамках данного параграфа мы раскроем содержание использования ресурсов сети «Интернет» при проведении соответствующей тактической операции. Реализация этого подхода позволяет с помощью ресурсов сети «Интернет» не только подтвердить факт события преступления, но и зафиксировать объективную связь между ним и проверяемым лицом.

В контексте изложенного также особую теоретическую и практическую сложность продолжает представлять проблема разграничения смежных составов преступлений, совершаемых с использованием сети «Интернет». Важным шагом на пути преодоления существующих правоприменительных коллизий стало принятие постановления Пленума Верховного Суда РФ от 15.12.2022 № 37, в котором были предложены доктринальные ориентиры относительно толкования категории «компьютерная информация», сущности нейтрализации средств защиты, момента окончания преступных деяний и специфики их квалификации в условиях использования сетевой инфраструктуры. На системный характер данных проблем также справедливо указывает Е. А. Русскевич, подчеркивая: экспоненциальное развитие информационно-коммуникационных технологий приводит к тому, что неправомерный доступ к компьютерной информации всё чаще выступает не изолированным деянием, а преобладающим способом совершения иных преступлений. Это существенно актуализирует потребность в выработке четких алгоритмов, позволяющих отграничивать преступления в сфере компьютерной информации от смежных посягательств, реализуемых посредством информационно-телекоммуникационных сетей[125].

Переходя к содержанию раскрытия преступления, следует отметить, что оно закономерно детерминировано ситуационными особенностями следственной

[125] См.: Русскевич Е. А. О совокупности преступлений в сфере компьютерной информации с другими преступлениями // Уголовное право. 2025. № 4. С. 76–84.

деятельности. В зависимости от того, из каких источников к следователю поступает первичная информация о преступлении, выделяют две типичные следственные ситуации, характерные для этапа возбуждения уголовного дела и определяющие дальнейший порядок получения уголовно-релевантной информации:

1. Информация о преступлении получена оперативным путем, материалы содержат достаточный объем сведений о событии преступления и лице, его совершившем (36,2 % изученных уголовных дел).

2. Информация о преступлении получена в ходе доследственной проверки по заявлению потерпевшего, есть достаточный объем сведений о событии преступления — чаще о его результате; сведения о лице, его совершившем, ограничены либо отсутствуют (52,4 % изученных уголовных дел).

Кроме того, могут иметь место типичные, но, по сравнению с вышеуказанными, относительно редко встречающиеся следственные ситуации:

3. Информация о преступлении получена по результатам случайных задержаний, сведения о преступлении ограничены, как правило, одним эпизодом, совершившее лицо задержано, есть отдельные данные о личности и его причастности (7,6 % изученных уголовных дел).

4. Информация о преступлении получена из другого уголовного дела (3,8 % изученных уголовных дел).

Каждая ситуация связана с решением определенных задач на этапе раскрытия.

Первая из указанных ситуаций определяет подзадачи установления непосредственного местонахождения заподозренного лица, получения сведений о возможных соучастниках и других эпизодах преступной деятельности, с поиском и фиксацией доказательств этих эпизодов.

Вторая ситуация определяет подзадачи установления личности лица, совершившего посягательство, и его местонахождения, поиска доказательств его непосредственного участия в преступлении.

В третьей ситуации возникают подзадачи установления преступного результата и потерпевшей стороны (не всегда значимо на первоначальном этапе,

когда потерпевшей стороной выступает государство), получения полных сведений о личности задержанного, установления его непосредственных действий в преступной деятельности, возможных соучастников.

В последней ситуации есть достаточно полная информация об одном из соучастников (в отношении которого расследовалось уголовное дело, из которого выделены материалы), требуется установить другие эпизоды и соучастников.

Как можно заметить, во всех ситуациях у следователя присутствует общая подзадача установления местонахождения конкретных лиц и неизвестных эпизодов (либо элементов) преступной деятельности.

На наш взгляд, решение этих задач возможно путем обращения следователя к ресурсам сети «Интернет» в двух указанных ранее формах: 1) как к источнику криминалистически значимой информации; 2) как к средству выявления (на этом этапе без фиксации и передачи) криминалистически значимой информации.

Если говорить об установлении события (или его отдельных элементов) преступления или неизвестных эпизодов преступной деятельности, использование сети «Интернет» как источника криминалистически значимой информации возможно в двух направлениях:

1) для установления латентного (зачастую совершаемого с использованием самой глобальной Сети) посягательства (или его эпизодов/элементов);

2) для получения дополнительной криминалистически значимой информации по очевидным преступлениям.

В настоящее время наблюдается явный уход криминальной активности из сети «Интернет» с открытым доступом в системы с ограниченным доступом и повышенным уровнем анонимности, например в «Даркнет». Поэтому в первом направлении обращение к Сети необходимо, как правило, оперативным путем в рамках оперативно-разыскной деятельности с привлечением соответствующих специалистов для анализа «Даркнета» и зашифрованных мессенджеров. По мнению А. Б. Смушкина, «для проникновения в сеть, изучения и изъятия информации в целях доказывания сотрудники правоохранительных органов

должны максимально использовать агентурные сети и легендированный ввод, внедрение сотрудника в число пользователей или получение доступа к учетной записи (логину и паролю) действующих пользователей»[126].

Необходимость использования возможностей оперативно-разыскной деятельности и специальных знаний в области компьютерных технологий с целью изучения зашифрованных ресурсов сети «Интернет» продиктована архитектурными особенностями данных пространств, основанными на криптографических методах защиты информации и обеспечивающими высокий уровень скрытности субъектов посягательства. Как уже указывалось в первой главе, «Даркнет» (как некое собирательное понятие) может быть основан на разных концепциях и технологиях. Наиболее известными являются системы Tor и I2P. Названные технологии используют многоуровневую криптографию, вследствие чего у заинтересованных структур, в том числе и правоохранительных, возникают сложности в расшифровке контента[127].

Объектами оперативного и следственного интереса в «Дарнете» могут выступать содержимое специализированных торговых площадок, реквизиты виртуальных финансовых активов, виртуальные следы коммуникации, идентификационные данные оборудования и устройств и т.д. К основным противозаконным сферам использования «Даркнета» ученые относят преступную деятельность, связанную с незаконным контентом сексуального характера, насилием, нарушением прав интеллектуальной собственности, оборотом наркотиков, компьютерной информации, поддельных банковских карт и их данных, поддельных документов, оружия, а также экстремистской направленности[128]. Поэтому большинство сайтов «Даркнета» представляют собой

---

[126] Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17. № 3. С. 105. DOI: 10.17803/1994-1471.2022.136.3.102-111.

[127] См.: Каримов В. Х. Актуальные вопросы выявления и расследования преступлений, совершаемых с использованием средств шифрования данных в сети Интернет // Уголовно-процессуальные и криминалистические чтения на Алтае. Проблемы противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами : сборник научных статей / отв. ред. С. И. Давыдов, В. В. Поляков. Вып. XIV. Барнаул : Изд-во Алт. ун-та, 2017. С. 40–47.

[128] См.: Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016.Т. 10. № 4. С. 651.

торговые площадки, на которых продавцы публикуют криминальные товары и услуги[129].

Впрочем, познание данных сторон криминальной деятельности вызывает определенные затруднения у правоохранительных органов. Мы разделяем позицию А. Б. Смушкина о низкой вероятности отработки всего массива лиц, входящих в «Даркнет». Проведение оперативно-разыскных мероприятий в отношении столь обширного массива лиц затруднительно в масштабах средних городов, а тем более крупнейших мегаполисов и городов федерального значения. Исходя из этого, следует делать акцент на ключевых субъектах: администраторе (собственнике) продающей нелегальный товар торговой площадки, продавце и покупателе товара. Здесь следует выделить два вектора оперативной и процессуальной работы: 1) от сайта торговой площадки или 2) от заказчика/покупателя. По первому как учеными, так и практиками предлагается в рамках оперативного эксперимента создание копий известных криминальных сайтов либо самостоятельных сайтов — торговых площадок для реализации криминальных товаров и услуг — с дальнейшим отслеживанием заказа и доставки или внедрением компьютерного червя при нематериальном информационном заказе в рамках контролируемой поставки[130].

Данная позиция подтверждается и проведенным обобщением правоприменительной практики. Например, в начале января 2022 г. сотрудниками ГУ МВД России по г. Москве проводился комплекс оперативно-разыскных мероприятий, направленных на установление лиц, занимающихся незаконным оборотом наркотических средств через интернет-магазин Cartel Contra El на торговой площадке Hydra. В ходе уголовного преследования и при заключении досудебных соглашений о сотрудничестве с задержанными владельцем и администратором интернет-магазина в рамках оперативного эксперимента регистрировались новые электронные торговые площадки, через которые были

[129] См., например: приговор Щелковского городского суда Московской области от 09.11.2025 по делу № 1-567/2025 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: https://sudact.ru (дата обращения: 22.06.2026).

[130] См.: Смушкин А. Б. Указ. соч.

установлены и привлечены к уголовной ответственности последующие изготовители и распространители наркотических средств[131].

По второму вектору, при поиске от заказчика, от клиента, А. Б. Смушкин рекомендует использовать информацию провайдера о подключении к входной ноде. «Может быть сопоставлено время выхода в «Даркнет», подключения к входной ноде и появления определенного преступного результата, преступного события»[132]. На наш взгляд, эффективность приведенных действий повышается, если уже есть заподозренный, действия которого отслеживаются оперативным путем. В отношении него устанавливается наблюдение, заказанные им предметы посягательства проверяются посредством контроля почтовых отправлений, телеграфных и иных сообщений.

Впрочем, с учетом системы шифрования теневых ресурсов, в частности «Даркнет», Hydra, помимо установления ранее неизвестного преступного события, на первый план выходит задача деанонимизации администраторов, продавцов и покупателей, о чем пойдет речь в следующем разделе исследования.

Второе направление получения криминалистически значимой информации по очевидным преступлениям представляет собой поиск информации, размещаемой на новостных сайтах, популярных развлекательных порталах, стриминговых сервисах и в мессенджерах. Очевидцы преступного события фиксируют его обстоятельства на мобильные телефоны и затем выкладывают записи в Сеть или транслируют в онлайн-режиме. Мало того что сами авторы размещенной информации являются прямыми свидетелями преступления, на их записях могут быть зафиксированы данные о других очевидцах, неустановленных соучастниках, предметах посягательства и орудиях преступления, способах сокрытия, расположенных в районе совершения посягательства средствах видео-, фотофиксации (банкоматы, домофоны и пр.) и т.п. Криминалистическая значимость такой информации обусловливается возможностью идентификации на

---

[131] См.: Уголовное дело № 1-333/2023 // Архив Красногорского городского суда Московской области ; уголовное дело № 1-541/2023 // Архив Одинцовского городского суда Московской области.

[132] Смушкин А. Б. Указ. соч.

видеозаписях лиц, причастных к преступлению, установления их ролей, а также фиксации динамики совершения посягательства, что в совокупности образует основу для последующего формирования доказательственной базы по уголовному делу.

Кроме того, такой сервис, как «Яндекс», аккумулирует данные о геопозиционировании устройств, находившихся в границах места совершения преступления в заданный период. Использование этих сведений позволяет следователю идентифицировать круг лиц, пребывавших в зоне происшествия, и установить маршруты их передвижения. Следует обратить внимание на то, что приложение «Яндекс Карты» показывает, в каких местах был владелец устройства, даже если он не искал эти места в навигаторе.

Возвращаясь к выделенной выше подзадаче установления местонахождения конкретных лиц, причастных к преступлению на этапе раскрытия преступления, следует учитывать, что каждый выход пользователя в сеть «Интернет» при помощи компьютера, смартфона, планшета и прочих цифровых устройств приводит к образованию следов его пребывания в Сети, пригодных для установления личности анонимного пользователя и построения маршрутов его передвижения на основе данных о точках доступа к телекоммуникационной сети.

Современные информационные технологии позволяют решать задачи жизнедеятельности человека путем непосредственной эксплуатации Сети самим пользователем либо генерирования необходимого результата цифровой технологии в автоматическом режиме по заранее разработанному алгоритму и предоставления его человеку. Вследствие этого в сети «Интернет» и устройствах доступа к ней образуется две группы следов в категории знаковых. Первая является пользовательской информацией, преобразованной электронно-вычислительным устройством, представленной в семантически понятном виде для человека и свидетельствующей о самом человеке и/или его деятельности. Такие следы могут быть информацией, распространение которой на территории Российской Федерации запрещено, а также сведениями, связанными с преступной деятельностью, или информацией о лице, причастном к преступлению,

выраженной в виде текстовых, табличных, графических, аудио- или видеоданных. Эта группа следов в связи с подготовкой, совершением или сокрытием преступления попадает в сферу внимания правоохранительных органов, как правило, в числе первых.

Ко второй группе следов относятся следы, алгоритмизированные в виде буквенно-цифрового кода, т.е. порождаемые электронными вычислительными устройствами, программным обеспечением, функционированием информационных систем, используемые для приема, передачи, доставки, обработки и хранения электронных сообщений и документов[133]. Как отмечают В. В. Поляков и А. В. Шебалин, компьютерные системы представляют собой совокупность технических и программных средств, используемых для формирования, приема, обработки, хранения, передачи и доставки информации. Эти средства связи представляют собой целостную электронно-вычислительную систему, в которой информация находится в электронно-цифровой форме, т.е. является компьютерной[134].

При этом первый и второй виды следов тесно взаимосвязаны и образуют сложную информационную систему. В то же время самым уязвимым элементом любой системы, как верно утверждает В. С. Овчинский, является сам человек[135]. Поэтому решение задачи по установлению пользователя сети «Интернет», по нашему мнению, должно быть основано в первую очередь на пользовательских и алгоритмизированных следах. Представляется, что формирование таких следов происходит уже на этапе подключения пользователя к сети «Интернет» посредством технического устройства. Такому сетевому подключению присваивается определенное символьное значение, называемое IP-адресом. Далее при переходе пользователя на какой-либо ресурс присвоенная символьная

---

[133] См.: Першин А. Н., Белова К. С. Криминалистические основы установления пользователя информационно-телекоммуникационной сети Интернет // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 82–94.

[134] См.: Поляков В. В., Шебалин А. В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2013. № 11-1. С. 123.

[135] См.: Овчинский В. С. Криминология цифрового мира : учебник для магистратуры. М. : Норма, Инфра-М, 2018. С. 154.

комбинация сохраняет свое значение и фиксируется на сервере провайдера, который обеспечивает подключение, и администратора того или иного интернет-ресурса.

Технологически IP-адрес представляет собой уникальный идентификатор (адрес) устройства, подключенного к сети «Интернет». То есть пользователь во время подключения к Сети уже будет представлен идентификатором — IP-адресом, который автоматически присваивается провайдером устройству, посредством которого пользователь подключается к Сети. Данный идентификатор скрыт от глаз пользователя. Для его обнаружения необходимо применить дополнительные манипуляции с устройством либо обратиться к провайдеру с запросом.

Соответственно, в ходе предварительного расследования для установления пользователя сети «Интернет» — физического лица — предстоит совершить последовательные действия: во-первых, установить идентификатор (IP-адрес); во-вторых, определить его соответствие использованному устройству; в-третьих, установить пользователя устройства, т.е. физическое лицо[136].

Пользователь сети «Интернет» осуществляет различные действия на ее ресурсах с присвоенным идентификатором: регистрацию на ресурсах, публикацию информации на них, пересылку файлов и другие различные действия. Кроме IP-адреса для осуществления таких действий необходимы дополнительные идентификаторы: доменное имя, сетевое имя пользователя, простая электронная подпись. Такие идентификаторы являются открытыми для широкой аудитории интернет-пользователей и не требуют дополнительных действий с устройством для их обнаружения.

В связи с этим необходимо уточнить, что входит в содержание понятия «идентификатор пользователя». Законодатель определяет идентификатор пользователя в коммуникационном интернет-сервисе как совокупность

---

[136] См., например: Сидорова К. С. Следственные ситуации и алгоритм их разрешения при установлении пользователя информационно-телекоммуникационной сети «Интернет» // Вклад Л. Я. Драпкина в криминалистическую науку : материалы Всероссийского научно-практического круглого стола (Екатеринбург, 1 ноября 2019 года). Екатеринбург : Уральский государственный юридический университет, 2019. С. 258–266.

информации (перечень критериев), присваиваемой при регистрации, на основании которой коммуникационный интернет-сервис идентифицирует (выделяет из числа иных пользователей) конкретного пользователя такого коммуникационного интернет-сервиса[137].

Следует отметить, что данное определение выработано применительно к такому интернет-ресурсу, как коммуникационный интернет-сервис. Однако ранее были обозначены идентификаторы пользователя, которые образуются не только в ходе работы с конкретным интернет-ресурсом, но и при подключении к сети «Интернет», что также позволяет установить пользователя.

В то же время, согласно техническому справочнику переводчика, идентификатор пользователя — это символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы[138]. По нашему мнению, данное определение является общим и не позволяет выявить специфику идентификаторов применительно к расследованию преступлений. Более того, с технической точки зрения нельзя сказать, что идентификатор присваивается только лицу или группе лиц. Соединение пользователя с сетью «Интернет» осуществляется посредством технического устройства, а один из вышеназванных идентификаторов задается именно сетевому подключению, а не физическому лицу.

В. В. Домарев, рассматривая понятие идентификатора пользователя, наполняет его более детальным содержанием: символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы, либо опознавание пользователя для определения его полномочий и прав на доступ к данным и выбора режима их использования. В данной дефиниции уделено внимание аспекту, связанному с опознаванием лица,

---

[137] Постановление Правительства РФ от 31.07.2014 № 759 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети “Интернет” информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети “Интернет” и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации».

[138] URL: https://technical_translator_dictionary.academic.ru/71328 (дата обращения: 03.10.2018).

использующего конкретный идентификатор, для определения юридических отношений между ними. По нашему мнению, это неслучайно, поскольку пользовательским идентификатором нелегально могло воспользоваться неопределенное количество людей, формально не связанных с ним. В связи с этим у правоохранительных органов может возникнуть версия относительно круга лиц, имеющих возможность воспользоваться идентификатором, которую в дальнейшем необходимо проверить.

В целом под идентификацией В. В. Домарев понимает присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов[139].

По мнению С. В. Зуева, идентификатор — это обозначаемый буквами ID программный элемент каскадных таблиц стилей, позволяющий назначать различный набор свойств одним и тем же физическим объектам HTML без использования классов. Такой идентификатор дает возможность определить любой компьютер, в том числе с помощью IP как уникального сетевого адреса узла в компьютерной сети[140].

На основании изложенного необходимо выделить основные, по нашему мнению, признаки идентификатора пользователя сети «Интернет»:

— идентификатор всегда представлен символьной комбинацией;

— идентификаторы могут не только присваиваться сетевому подключению посредством пользовательского оборудования, но и самостоятельно задаваться пользователем на конкретном ресурсе сети «Интернет»;

— идентификаторы позволяют определить техническое оборудование и данные лица, которое юридически имело право его использовать.

Изложенное позволяет сделать вывод о том, что идентификатором пользователя сети «Интернет» является присваиваемая сетевому подключению или задаваемая пользователем уникальная комбинация символов, позволяющая

---

[139] См.: Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Киев : ТИД ДС, 2002. С. 630.

[140] См.: IT-справочник следователя / под ред. д-ра юрид. наук С. В. Зуева. М. : Юрлитинформ, 2019. С. 40.

в процессе раскрытия и расследования преступлений выделять конкретное лицо или оконечное оборудование из неопределенного круга, устанавливать устойчивую связь между виртуальным образом и реальным субъектом, а также документально фиксировать факты присутствия и выполнения отдельных операций в информационно-телекоммуникационной сети «Интернет».

Руководствуясь определением идентификатора пользователя, спецификой функционирования, считаем возможным разделить перечисленные идентификаторы — IP-адрес, никнейм/логин, доменное имя — на две группы:

— «видимые» идентификаторы — доменное имя, сетевое имя пользователя, простая электронная подпись;

— «невидимые» идентификаторы — IP-адрес.

Идентификаторы — сетевое имя пользователя, доменное имя — являются открытыми и общедоступными в сети «Интернет», их видят пользователи Сети, и для этого не требуется применения глубоких (специальных) знаний из области функционирования компьютерных технологий. Выявить и исследовать «видимые» идентификаторы может следователь самостоятельно, без совершения процессуальных действий, связанных с направлением запросов в соответствующие организации. По нашему мнению, такое разделение может быть обоснованным и целесообразным с точки зрения специфики функционирования идентификаторов и использования сведений о них для идентификации физического лица[141].

В то же время необходимо отметить: имеющиеся научные и практические разработки в области традиционной теории криминалистической идентификации[142] не в полной мере позволяют отождествить человека с

---

[141] См., например: Сидорова К. С. Использование следователем (дознавателем) идентификаторов личности в сети Интернет // Преемственность и новации в юридической науке : материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей (Омск, 20 марта 2018 г.) / отв. за вып. канд. юрид. наук И. В. Сидорова. Омск : Омская академия МВД России, 2018. Вып. 14. С. 102–104 ; Она же. Особенности установления сведений о пользователе информационно-телекоммуникационной сети «Интернет» в расследовании преступлений // Совершенствование уголовно-процессуальных и криминалистических мер противодействия преступности : материалы международной научно-практической конференции (26 ноября 2021 г.) / пред. редкол. М. М. Горшков. Омск : Омская академия Министерства внутренних дел РФ, 2022. С. 89–91.

[142] См., например: Колдин В. Я. Идентификация и ее роль в установлении истины по уголовным делам. М. : Изд-во Моск. ун-та, 1969 ; Колмаков В. П. Идентификационные действия следователя. М. : Изд-во Моск. ун-та, 1977 ; Потапов С. М. Принципы криминалистической идентификации // Советское государство и право. 1940. № 1. С. 66–81 ; Седова Т. А. Проблемы методологии и практики нетрадиционной криминалистической идентификации.

пользователем сети «Интернет» при помощи вышеназванных идентификаторов. Это связано с тем, что преступникам, использующим сеть «Интернет», свойственно стремление свести к минимуму возможность установления их личности, оставаясь максимально не замеченными в Сети. Это происходит неслучайно, поскольку использование сети «Интернет» в полной мере нормативно не урегулировано действующим законодательством. Кроме того, есть и различные программные средства, позволяющие осуществлять действия в Сети анонимно, используя так называемые анонимайзеры[143]. В связи с этим нельзя не согласиться со Г. В. Скорик в том, что не всегда реальная и виртуальная идентичности совпадают[144].

Согласно постановлению Правительства РФ от 31.07.2014 № 758 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона “О внесении изменений в Федеральный закон ‘Об информации, информационных технологиях и о защите информации’ и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей”» оказание универсальных услуг связи по передаче данных и предоставлению доступа к сети «Интернет» с использованием пунктов коллективного доступа осуществляется оператором универсального обслуживания после проведения идентификации пользователей. Последняя реализуется оператором универсального обслуживания путем установления фамилии, имени, отчества (при наличии) пользователя, подтверждаемых документом, удостоверяющим личность. Помимо этого, согласно Указу Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» для развития сети «Интернет» и информационной инфраструктуры Российской Федерации необходимо проводить мероприятия на международном уровне, в частности создавать новые механизмы партнерства,

---

Л. : Изд-во Ленингр. ун-та, 1986 ; Степаненко Д. А. Проблемы теории и практики криминалистической идентификации : дис. … д-ра юрид. наук. Иркутск, 2006 и др.

[143] См.: Вехов В. Б., Ульянова М. А. К вопросу криминалистического исследования анонимайзеров // Актуальные научные исследования в современном мире. 2018. № 7-3. С. 54–57.

[144] См.: Скорик Г. В. Человек в информационном обществе: проблема идентификации (поиска идентичности) // Вестник Томского государственного университета. 2007. № 302. С. 55.

призванные с участием всех институтов общества выработать систему доверия в сети «Интернет», гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации, исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в сети «Интернет». А одним из основных направлений развития российских информационных и коммуникационных технологий являются доверенные технологии электронной идентификации и аутентификации.

Следует отметить, что одной из задач Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 № 646, является исключение анонимности человека в сети «Интернет». Воплощением данной Доктрины в жизнь государством стали принятие целого ряда новых и совершенствование существующих нормативных правовых актов, касающихся урегулирования процедуры идентификации пользователя в информационно-телекоммуникационных сетях. Так, например, пункт 1 ч. 4.2 ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» обязывает организатора распространения информации в сети «Интернет» осуществлять «идентификацию пользователей сети “Интернет”, передачу электронных сообщений которых осуществляет организатор сервиса обмена мгновенными сообщениями по абонентскому номеру оператора подвижной радиотелефонной связи».

Доступ пользователей к информации, содержащейся в государственных информационных системах и иных информационных системах, осуществляется через Единую систему идентификации и аутентификации (ЕСИА)[145]. Для получения учетной записи в ЕСИА необходимо удостоверить свою личность с

[145] Регламентируется постановлением Правительства РФ от 28.11.2011 № 977 «О Федеральной государственной информационной системе “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме”». Виды идентификаторов определяются в соответствии с постановлением Правительства РФ от 14.09.2012 № 928 «О базовых государственных и информационных ресурсах» и Положением о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (утв. приказом Минкомсвязи России от 13.04.2012 № 107).

помощью паспортных данных, ИНН и СНИЛС, а также номера мобильного телефона и адреса электронной почты, являющихся идентификаторами сведений о субъектах доступа (физических и юридических лицах)[146].

В соответствии с постановлением Правительства РФ от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи» в случае заключения срочного договора об оказании разовых телематических услуг связи в пунктах коллективного доступа оператор связи осуществляет идентификацию пользователей и используемого ими оконечного оборудования[147].

Идентификация пользователя осуществляется оператором связи путем установления фамилии, имени, отчества (при наличии) пользователя, подтверждаемых документом, удостоверяющим личность, либо иным способом, обеспечивающим достоверное установление указанных сведений, в том числе с использованием ЕСИА, или достоверного установления абонентского номера, назначенного пользователю в соответствии с договором об оказании услуг подвижной радиотелефонной связи, заключенным с оператором связи.

Идентификация оконечного оборудования реализуется средствами оператора связи путем определения уникального идентификатора оборудования сетей передачи данных.

Более того, согласно данному постановлению оператор связи может потребовать подтвердить соответствие персональных данных фактического пользователя сведениям, заявленным в договоре, осуществить подтверждение персональных данных путем представления оператору связи документа, удостоверяющего личность, или иным указанным способом.

Кроме того, о способах идентификации упоминается в Федеральном законе «О связи», постановлении Правительства РФ от 16.07.2007 № 447 «О совершенствовании учета федерального имущества» и др.

---

[146] Постановление Правительства РФ от 12.08.2014 № 801 «О внесении изменений в некоторые акты Правительства Российской Федерации» // СПС «КонсультантПлюс».

[147] Оператор связи оказывает телематические услуги связи, в том числе доступа к сети «Интернет», на основании договора.

В руководящем документе «Защита от несанкционированного доступа к информации. Термины и определения» под идентификацией понимается присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Расшифровывается термин «идентификатор доступа» как уникальный признак субъекта или объекта доступа[148].

Помимо этого, в настоящее время идет активное внедрение системы цифрового профиля граждан России и иностранных граждан, под которым понимается совокупность сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих отдельные публичные полномочия, а также в ЕСИА[149]. Полагаем, что с целью идентификации лица также возможно производить так называемую привязку цифрового профиля лица путем его синхронизации с используемыми им электронными средствами коммуникации, например с мессенджерами.

Исходя из вышеизложенного, следует отметить, что государственные меры, принимаемые для исключения анонимности пользователя в Сети, позволяют до определенной степени воспринимать след в сети «Интернет» как отражение человека с его истинными данными.

Впрочем, использование сетевых технологий в раскрытии и расследовании преступлений свидетельствует о том, что в процессе установления физического лица — пользователя сети «Интернет» — через идентификаторы следует учитывать: пользовательским оборудованием, которому был присвоен идентификатор в Сети, мог воспользоваться широкий круг лиц. Поэтому полагаем, что процесс сопоставления идентификатора пользователя сети «Интернет» с

---

[148] Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением председателя Гостехкомиссии России от 30.03.1992) [Электронный ресурс] // ФСТЭК России : официальный сайт. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2 (дата обращения: 03.10.2022).

[149] См.: Законопроект № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» [Электронный ресурс] // URL: https://sozd.duma.gov.ru/bill/747513-7 (дата обращения: 23.11.2024).

реальным человеком подразумевает проведение комплекса следственных действий и оперативно-разыскных мероприятий для установления лица, использовавшего оборудование с таким идентификатором в интересующий следствие момент, т.е., как отмечает Г. В. Скорик, сочетание реального и виртуального способов идентификации[150].

Если в классической версии человека можно однозначно идентифицировать по следу руки, который он оставил на месте происшествия, при этом изучая как можно больше его частных признаков, то по следу в сети «Интернет» также возможно говорить об индивидуальной идентификации, но не исключая вероятный групповой характер. В данном контексте объектами групповой идентификации могут являться как законный владелец технического устройства, так и иные лица, которые могли иметь к нему доступ.

Соответственно, минимумом признаков, достаточных для решения вопроса об идентификации, могут быть IP-адрес, MAC-адрес, IMEI[151], логин.

Считаем, что первоначальный алгоритм действий субъектов уголовного преследования по решению задачи, связанной с установлением информации о посягательстве, позволяющей квалифицировать его как преступление, и совершившем его лице, путем соотнесения пользовательских идентификаторов с конкретным человеком может быть следующим.

1. Выяснение идентификатора пользователя.

2. Подготовка и направление запроса организатору распространения информации в сети «Интернет» (провайдеру связи, администратору сайта) с целью получения более подробной информации по интересующему идентификатору и устройству, осуществлявшему доступ в сеть «Интернет». Получение такой информации возможно в рамках проведения следственного действия, предусмотренного статьей 186.1 УПК РФ («Получение информации о соединениях между абонентами и (или) абонентскими устройствами»).

---

[150] См.: Скорик Г. В. Указ. соч. С. 55.

[151] В данный момент разрабатываются поправки к Федеральному закону «О связи», согласно которым будет осуществляться привязка сим-карт к конкретным устройствам по коду IMEI, т.е. оператора связи обяжут проверять, в каком именно устройстве используется SIM-карта, и фиксировать эти данные.

3. Допрос владельца пользовательского оборудования.

4. Установление круга лиц, имеющих доступ к пользовательскому оборудованию, их допрос[152].

5. Осмотр и анализ документа, полученного в порядке ст. 186.1 УПК РФ по номерам телефонов лиц, имеющих доступ к пользовательскому оборудованию, и их анализ с позиции их местонахождения в интересующий момент входа в сеть «Интернет» с конкретного устройства.

6. Выемка и осмотр видеозаписей вблизи того географического места, откуда осуществлялось подключение к сети «Интернет», для отслеживания местоположения лиц, имевших доступ в Сеть в интересующий следователя момент.

7. Обыск места, откуда пользователем производился доступ в сеть «Интернет».

8. Осмотр пользовательского оборудования.

9. Назначение экспертиз (компьютерно-технической, лингвистической и пр.)[153].

Среди оперативно-разыскных мероприятий, направленных на установление пользователя сети «Интернет», причастного к совершению преступлений, можно указать следующие:

1. Наведение справок, предполагающее получение из различных учреждений сведений о пользователе, а также данных из открытых источников информационных ресурсов.

---

[152] См., например: Сидорова К. С. Обстоятельства, выясняемые у подозреваемого (обвиняемого) в ходе допроса об использовании им коммуникационных технологий через сеть интернет // Преемственность и новации в юридической науке : материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей (Омск, 28 марта 2017 г.) / отв. за вып. канд. юрид. наук И. В. Сидорова. Омск : Омская академия МВД России, 2017. Вып. 13. С. 86–88.

[153] Более подробно данный вопрос рассмотрен в работах: Першин А. Н., Сидорова К. С. Криминалистические основы установления пользователя информационно-телекоммуникационной сети Интернет // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3 (55). С. 82–94 ; Сафронов Д. М., Сидорова К. С. Уголовно-процессуальные и криминалистические аспекты получения информации о пользователях сети Интернет при производстве следственных действий // Российская юстиция. 2021. № 1. С. 30–33.

2. Сбор образцов для сравнительного исследования, предполагающий получение объектов — носителей информации, необходимых для их исследования путем изучения, описания, сравнения с ранее добытыми объектами.

3. Получение компьютерной информации.

4. Наблюдение — оперативно-разыскное мероприятие, осуществляемое в сетях передачи информации с использованием специальных технических средств (возможно использование программного комплекса «Мобильный криминалист», позволяющего извлекать, расшифровывать и анализировать данные (в том числе удаленные) из облачных хранилищ, мессенджеров, почтовых сервисов, веб-браузеров, исследовать коммуникации между несколькими устройствами[154]) и с фиксацией / без фиксации результатов для получения сведений, имеющих значение для решения задач оперативно-разыскной и уголовно-процессуальной деятельности.

5. Оперативное внедрение, открывающее широкие возможности для обнаружения, изучения, фиксации информационных объектов.

6. Оперативный эксперимент, направленный на моделирование определенных информационных объектов и отношений, возникающих в противоправных действиях субъектов Сети.

7. Проверочная закупка, позволяющая определить добровольность и осведомленность владельцев и пользователей сайтов при осуществлении преступной деятельности через интернет-ресурсы.

8. Контролируемая поставка при получении заказа на предметы преступной деятельности и последующей их доставке.

Следует отметить, что перечень оперативно-разыскных мероприятий, которые необходимо провести в рамках расследуемого преступления, будет варьироваться в зависимости от сложившейся следственной ситуации путем увеличения или уменьшения их количества.

---

[154] См.: Мобильный Криминалист [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/Продукт:Мобильный_Криминалист (дата обращения: 07.11.2024).

Таким образом, при успешном взаимодействии следственных и оперативных подразделений, тактически верном разделении обязанностей по поставленным задачам, а также умелом использовании интернет-ресурсов становится возможным решить задачу, связанную с установлением лица, совершившего преступное посягательство, и признаков состава преступления в его действиях. Безусловно, количество и порядок осуществления следственных действий и оперативно-разыскных мероприятий будут зависеть от сложившейся следственной ситуации по делу в целом и варьироваться исходя из объема имеющихся данных. При этом в процессе разрешения данной задачи возможно и необходимо производить идентификацию пользователей сети «Интернет» путем применения комплекса мер по их деанонимизации, направленных на преодоление используемых средств скрытия сетевой активности и установление связи между виртуальным цифровым профилем и конкретным физическим лицом.

## § 2. Изучение личности совершившего преступление, его розыск и изобличение с использованием ресурсов сети «Интернет»

Криминалистическому изучению личности учеными уделено значительное внимание на диссертационном и монографическом уровнях[155]. Однако большинство исследований проведено в период до наступления эры всеобщей цифровизации. Поэтому аспекты изучения личности посредством обращения к ресурсам сети «Интернет» в настоящее время представлены разрозненными публикациями в сборниках научных трудов, периодических изданиях и на

[155] См.: Ведерников Н. Т. Личность обвиняемого и подсудимого (понятие, предмет и методика изучения). Томск, 1978 ; Глазырин Ф. В. Изучение личности обвиняемого и тактика следственных действий. Свердловск, 1973 ; Центров Е. Е. Криминалистическое учение о потерпевшем. М. : Изд-во Московского ун-та, 1988 ; Жбанков В. А., Меглицкий Г. Н. Криминалистические средства и методы установления лиц, совершивших преступления. М., 1993 ; Образцов В. А. Выявление и изобличение преступника : учебное пособие. М. : Юрист, 1997 ; Ахмедшин Р. Л. Изучение личности преступника в методике расследования преступлений. Томск, 2000 ; Демидов Н. Н. Изучение личности преступника в процессе расследования : дис. … канд. юрид. наук. Волгоград, 2003 ; Макаренко И. А. Личность несовершеннолетнего обвиняемого как объект криминалистического исследования. М. : Юрлитинформ, 2006 ; Малыхина Н. И., Повезнюк Г. И. Криминалистические методы и средства установления личности в процессе расследования преступлений. По материалам стран СНГ. М. : Юрлитинформ, 2005 и др.

электронных ресурсах самой глобальной Сети[156]. В их числе особый интерес представляет работа Н. В. Олиндер и Е. А. Гамбаровой, опубликованная по результатам их экспериментальных исследований на базе юридического факультета Самарского национального исследовательского университета[157].

Указанные ученые для разработки рекомендаций по использованию в расследовании социальных медиа, под которыми они понимают интернет-сообщества, блоги, виртуальные игры, социальные сети, сообщества по производству совместного контента, совместные проекты и геосоциальные сервисы, в рамках эксперимента дали задание студентам по сбору информации о людях посредством социальных медиа и традиционного опроса. В результате сбор информации посредством сети «Интернет» оказался почти в 10 раз быстрее традиционных способов опроса. Объем полученных сведений также был значительно больше и разнообразнее. По результатам исследования ими был предложен алгоритм сбора информации из социальных медиа, включающий:

«1. Запрос о человеке в поисковых системах Google и Yandex по фамилии, имени, отчеству.

2. Использование сайта «Яндекс.Люди».

3. Поиск по номеру телефона и по адресу электронной почты.

4. Поиск информации на сайте ГАИ, ФССП, налоговой.

5. Поиск по фото.

6. Поиск информации напрямую через социальные сети»[158].

---

[156] См.: Протасевич А. А., Фойгель Е. И. Методология криминалистического учения о человеке и человеческой деятельности // Всероссийский криминологический журнал. 2017. Т. 11. № 3. С. 596 ; Хомяков Э. Г. Электронная медицинская карта как источник разыскной и криминалистически значимой информации при расследовании преступлений, связанных с безвестным исчезновением граждан // Раскрытие и расследование преступлений, связанных с безвестным исчезновением граждан : материалы международной научно-практической конференции. М., 2018. С. 223–226 ; Каминский А. М., Овчинникова Д. А. Использование электронных криминалистически неупорядоченных банков данных в раскрытии преступлений // Вестник Удмуртского университета. 2020. Т. 30. Вып. 1. С. 91–98 ; Романова Л. И. Личность интернет-преступника // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 159–169 ; Левгеева Т. Б. Криминалистический анализ личности преступника, совершившего преступление с использованием интернет-технологий // Исследования молодых ученых : материалы XXX Международной научной конференции, г. Казань, январь 2022 г. Казань : Молодой ученый, 2022. С. 33–36 и др.

[157] См.: Олиндер Н. В., Гамбарова Е. А. Проблемные вопросы поиска и восприятия информации о человеке в сети Интернет и ее использование при расследовании преступлений // Юридический вестник Самарского университета. 2016. Т. 2. № 4. С. 55–59.

[158] См.: Олиндер Н. В., Гамбарова Е. А. Указ. соч. С. 58.

В социальных сетях ими предлагается идти по пути поиска соответствующей страницы, ее анализа (изучения открытой информации, просмотра фотографий, комментариев), поиска по «лайкам», сторонних ссылок, общих друзей[159].

Впрочем, предложенный несложный алгоритм указывает, что авторы выходят за границы определенных ими видов социальных медиа и предлагают также обращаться к официальным базам данных государственных органов (при этом их список не отличается широтой). На наш взгляд, при построении подобного алгоритма целесообразно отдельно показать правоприменителю возможности установления сведений о человеке, его розыска и изобличения в совершении преступления как путем обращения к упомянутому в предыдущем параграфе цифровому профилю, поиска в социальных сетях и мессенджерах, так и путем розыска на официальных сайтах органов государственной власти и проверки полученных сведений[160].

В цифровой профиль гражданина попадает только актуальная и проверенная информация из регистров большинства государственных органов[161]. Анализ таких сведений позволяет следователю своевременно проверять выдвинутые версии относительно преступления, оперативно устанавливать фактическое местонахождение лица, а также качественно осуществлять подготовку к следственным действиям с его участием (например, к допросу).

Постановлением Правительства РФ от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» определено, какие организации и для каких целей могут получить доступ к цифровым профилям граждан[162]. В большинстве случаев сведения из цифрового профиля запрашивают нижеперечисленные организации для следующих целей:

---

[159] Олиндер Н. В., Гамбарова Е. А. Указ. соч. С. 58.

[160] См., например: Павлов А. В., Сидорова К. С. Получение и использование сведений с сайтов социальных интернет-сетей для установления местонахождения подозреваемого (обвиняемого), находящегося в розыске // Законодательство и практика. 2017. № 1 (38). С. 14–16.

[161] В приложении 2 приводятся наиболее востребованные сведения из цифрового профиля гражданина РФ, которые можно получить с помощью веб-модуля «RS-Connect. Цифровой профиль».

[162] СЗ РФ. 2019. № 23. Ст. 2963.

— кредитные организации — для оформления заявок на кредит, выдачи банковских карт и других действий;

— страховые компании — для подписания договоров страхования, оформления заявок на страховые выплаты и других действий;

— операторы сотовой связи — для заключения договоров с абонентами;

— Агентство по страхованию вкладов — для оформления заявок на страховые выплаты в случае банкротства банка;

— бюро кредитных историй — для запроса отчетов по истории кредитов гражданина;

— железнодорожные и авиаперевозчики — для продажи билетов;

— работодатели — для заключения трудовых договоров[163].

Соответственно, названные организации могут рассматриваться как самостоятельные источники сведений о субъекте. Вместе с тем первичная идентификационная информация в этом случае дополняется специфическими данными, отражающими характер взаимодействия лица с конкретной организацией-источником. С целью получения и закрепления таких сведений необходимо производить выемку соответствующих документов и носителей информации, их последующий осмотр, а в случае необходимости — назначать судебные экспертизы. Наличие указанных данных позволяет устанавливать круг связей интересующего лица, его фактическое местонахождение на основе последних транзакций с использованием электронных средств платежа. Это способствует эффективному выстраиванию и проверке следственных версий, а также сбору характеризующего материала для качественной подготовки к проведению следственных действий, в частности допроса.

Далее переходим к особенностям поиска и получения информации из социальных сетей и мессенджеров. Под социальной сетью понимается интернет-площадка, сайт, который позволяет зарегистрированным на нем пользователям

[163] См.: Лопатина В. Цифровой профиль гражданина: что это и чем полезен организациям [Электронный ресурс] // URL: https://www.softlab.ru/blog/citizen-digital-profile (дата обращения: 11.11.2024).

размещать информацию о себе и общаться, устанавливая социальные связи[164]. Наиболее популярными социальными сетями являются «ВКонтакте», «Одноклассники», TenChat, Instagram[165] и т.д.

Ввиду того, что цифровая среда очень динамична и быстро меняется с каждым годом, за время написания этой работы могли появиться новые социальные сети, а некоторые из существующих — прекратить функционировать. Правоприменителю необходимо уяснить, что принцип действия у всех социальных сетей примерно одинаков, а их содержание позволяет получить всевозможную информацию о личности интересующего следствие лица.

Как социальные сети, так и мессенджеры предназначены для коммуникации. Однако у первых более широкий набор функций: они сочетают в себе чат, сервис знакомств, новостную ленту и личный блог в одном приложении. В социальных сетях можно общаться через открытые сообщества, публиковать записи, выкладывать фото и видео, слушать музыку. Некоторые социальные сети выпускают отдельные приложения-мессенджеры, связанные с основным сайтом. Мессенджеры предназначены для приватного общения между несколькими людьми. Эти приложения не перегружены другими функциями, а потому их часто используют для работы, чтобы не отвлекаться на новостную ленту и развлекательный контент. Однако в популярных мессенджерах тоже есть сообщества по интересам.

К числу самых популярных мессенджеров относятся Max, VK-мессенджер, Telegram, WeChat, Snapchat и т.д.

Анализ этих сведений позволяет решать задачи, связанные с восстановлением хронологии преступного события, поиском похищенного имущества, а также задачи по соотнесению идентификатора пользователя с конкретным физическим лицом, установлению круга соучастников.

---

[164] См.: Безопасность пользователей в сети Интернет [Электронный ресурс] // URL: https://safe-surf.ru/users-of/article/228/ (дата обращения: 10.03.2025).

[165] Необходимо отметить, что деятельность социальной сети Instagram (принадлежит компании Meta) признана экстремистской, а доступ к данному ресурсу ограничен на основании решения суда, однако он продолжает выступать в качестве востребованного канала коммуникации и площадки для размещения контента.

В минимальный объем сведений, по которым возможно отыскать и в дальнейшем идентифицировать интернет-пользователя, входят фамилия, имя; пол; дата рождения, место рождения; номер мобильного телефона / адрес электронной почты; ID (идентификационный номер) / логин[166] / никнейм; фотография с четким изображением лица (при наличии).

Такие исходные данные для поиска лица на сайтах социальных сетей или мессенджеров могут быть достаточными для его успешного отыскания. При необходимости может потребоваться и другая информация, например семейное положение, место учебы/работы, образование, паспортные данные, наличие судимости и т.д. В этом случае появляется вероятность успешного отыскания более подробных сведений о лице после установления его места пребывания на каких-либо ресурсах[167], что будет способствовать познанию лица с разных сторон.

Проведенный анализ информации о пользователях сайтов социальных сетей, которую можно использовать для решения задач установления сведений о личности преступника, его розыска и изобличения, показал, что ее можно подразделить на:

— информацию, которую пользователь указывает о себе самостоятельно (например, в ходе регистрации, а также дополнительные данные, указываемые в разделах аккаунта);

— информацию, отражающую техническую сторону подключения пользователя к социальной сети, а также личную переписку и иные сведения, которые хранятся у организатора распространения информации, в частности у администратора сайта социальной сети (например, данные о фактах авторизации)[168].

---

[166] Логин (login) — имя (идентификатор) учетной записи пользователя в компьютерной системе (URL: https://ru.wikipedia.org/wiki/Логин (дата обращения: 23.09.2023)).

[167] Место пребывания на ресурсах сети «Интернет» понимается как обращение, совершение каких-либо действий пользователем на них.

[168] См. подробнее об этом: Першин А. Н., Сидорова К. С. Использование ресурсов информационно-телекоммуникационной сети «Интернет» в розыскной деятельности следователя // Библиотека криминалиста. 2017. № 4. С. 320–325 ; Сидорова К. С. Направления поисковых действий следователя в информационно-телекоммуникационной сети «Интернет» при расследовании преступлений. С. 135–143.

Таким образом, следователь имеет возможность самостоятельного получения каких-либо сведений об интересующем лице, только если оно является зарегистрированным пользователем сайта какой-либо социальной сети. Объем полученной информации о пользователе будет зависеть от того, какие ограничения в отношении доступности своих личных данных установил последний.

Следует отметить, что информацию о пользователе возможно получить не только самостоятельно, исследовав его аккаунт в Сети, но и посредством взаимодействия с администрацией соответствующего сайта. Переписка пользователя с другими пользователями, сведения о фактах авторизации (данные о технических средствах (устройствах), технологическом взаимодействии с сайтом (в том числе IP-адрес хоста, вид операционной системы пользователя, тип браузера, географическое положение, поставщик услуг сети «Интернет», данные из адресной книги)) имеются у организатора распространения информации, в частности у администратора того или иного сайта. Такие сведения следователь может получить только через администрацию сайта в сети «Интернет» при наличии мотивированного запроса и постановления суда о разрешении получения соответствующей информации, поскольку она отражает персональные данные лица.

Важно отметить, что у каждого сайта социальной сети имеется сервер[169], одной из задач которого является хранение данных (например, адреса электронной почты пользователя, личных данных, данных о технологическом взаимодействии пользователя с сайтом и т.д.). Для получения более подробных сведений о пользователе необходимо направлять мотивированный запрос организатору распространения информации в сети «Интернет» — администратору сайта социальной сети. Практика расследования уголовных дел складывается таким образом, что администраторы сайтов, серверы которых расположены в пределах Российской Федерации, беспрепятственно направляют правоохранительным органам интересующую их информацию о пользователе по запросу. Сложнее дело

[169] См.: Сервер [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Сервер_(аппаратное_обеспечение) (дата обращения: 24.09.2023).

обстоит с получением сведений о российском гражданине, который зарегистрирован на сайте социальной сети, сервер которого расположен на территории иностранного государства (например, сервер мессенджера WhatsApp находится в США), в связи с чем усложняется процедура получения информации с таких сайтов (необходимо направлять международный запрос). Как показывает практика расследования, ответы на подобные запросы поступают либо очень долго (от года и больше), либо не поступают вообще. В связи с этим реализуется комплекс мер по обеспечению серверных мощностей в пределах юрисдикции Российской Федерации, расширению сегмента отечественных интернет-ресурсов и исключению анонимизации пользователей в сети «Интернет».

На наш взгляд, данные о пользователе, полученные следователем с сайтов социальных сетей в ходе поисково-познавательной деятельности, будут благоприятным образом влиять на ход расследования путем пополнения сведений о самом подозреваемом (обвиняемом), а информация о технической стороне взаимодействия пользователя с сайтом даст возможность установить физическое место нахождения лица. Эти меры позволят сократить количество уголовных дел, приостановленных из-за того, что подозреваемый или обвиняемый скрылся от следствия либо место его нахождения не установлено по иным причинам (п. 2 ч. 1 ст. 208 УПК РФ).

Далее, анализируя функциональные возможности мессенджеров, мы пришли к выводу, что при наличии номера интересующего абонента (подозреваемого, обвиняемого) и при условии его регистрации в каком-либо мессенджере следователь способен установить факт использования подозреваемым (обвиняемым) конкретной программы по мгновенному обмену сообщениями. В таком случае можно отследить динамику появления абонента в Сети, фотографии его профиля, а также самостоятельно либо с помощью иных подразделений выйти с ним на контакт.

Следует отметить, что с 1 марта 2022 г. в России вступили в силу Правила идентификации в мессенджерах через мобильных операторов, регламентируемые постановлением Правительства РФ от 20 октября 2021 г. № 1801 «Об утверждении

Правил идентификации пользователей информационно-телекоммуникационной сети “Интернет” организатором сервиса обмена мгновенными сообщениями». Если данные, которые лицо указывало при регистрации в мессенджере, совпадут с данными, имеющимися у оператора связи по соответствующему абонентскому номеру, то пользователь сможет пройти авторизацию, после чего получит уникальный номер. Его внесут в специальный реестр оператора с указанием, каким именно сервисом пользуется клиент.

Впрочем, в этой части есть и проблемные моменты, с которыми сталкиваются сотрудники правоохранительных органов при раскрытии и расследовании преступлений. В большинстве современных мессенджеров используется сквозное шифрование, при котором данные на оконечных устройствах преобразуются и становятся недоступными для организаторов распространения информации в сети «Интернет», т.е. данные остаются доступными только на устройстве пользователя, что существенно осложняет порядок получения криминалистически значимых сведений. В этой связи представляется целесообразным сосредоточить внимание на анализе цифрового профиля лица и поиске информации в других открытых интернет-источниках.

Таким образом, получение следователем интересующей его информации предполагает несколько вариантов действий: направление запроса оператору связи и самостоятельный поиск по всем известным мессенджерам. Следует отметить, что, действуя в рамках первого варианта, следователь имеет возможность извлечь информацию в большем объеме, а именно узнать дату установки мессенджера, его удаления, получить сведения об авторизации или деавторизации, об абоненте — пользователе мессенджера (установить его фамилию, имя, отчество, дату, место рождения). Полагаем, что следователю не стоит пренебрегать таким источником информации, как мессенджер, поскольку необходимо использовать все доступные средства и способы с целью обнаружения сведений об искомом лице.

Высокая степень интеграции персональных электронных устройств в повседневную жизнедеятельность человека обуславливает их неразрывную пространственно-временную связь с личностью владельца. Данное обстоятельство

позволяет решать задачу розыска и изобличения лица в причастности к совершению преступления путем соотнесения IP-адресов используемых технических средств и последующего анализа зафиксированной сетевой активности в привязке к географическим координатам субъекта.

В результате подключения к сети «Интернет» посредством технического устройства физическое лицо представляется нам пользователем этой сети, а техническому устройству, регистрирующемуся в ней, присваивается конкретный идентификатор — IP-адрес, позволяющий отличить такое подключение от других. Соответственно, на серверах происходит процесс отражения действий пользователя в сети «Интернет» при использовании в подключении к Сети конкретного IP-адреса, присвоенного провайдером, в виде следовой картины, установление элементов которой имеет значение для успешного расследования преступления[170].

Помимо того, что следователю необходимо установить техническое устройство, с которого физическим лицом осуществлялся доступ в сеть «Интернет», следует доказать, что конкретное лицо осуществляло определенные действия, используя сеть «Интернет» и ее ресурсы с этого устройства, а также, возможно, маскировало свои действия — применяло различные сервисы по анонимизации своей деятельности в Сети[171].

Тем самым для того, чтобы идентифицировать конкретное лицо в сложной цепочке («физическое лицо → техническое оборудование → подключение к сети “Интернет” → результат действий на определенном ресурсе сети “Интернет” — правомерное или противоправное деяние»), необходимо произвести комплекс технических, организационных и тактических мер путем осуществления следственных действий и оперативно-разыскных мероприятий.

---

[170] Более подробно данный вопрос рассмотрен в работах: Сидорова К. С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. 2018. № 3 (74). С. 84–87 ; Она же. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2 (26). С. 88–92.

[171] См., например: Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : учебник : в 2 ч. / Гаврилин Ю. В., Пинкевич Т. В., Мартыненко Н. Э. [и др.] ; под общ. ред. Ю. В. Гаврилина. М. : Академия управления МВД России, 2024. Ч. 1.

Более того, установив связь такого идентификатора, как IP-адрес, с техническим устройством, а затем и с физическим лицом, с которым провайдер заключил договор об оказании услуг связи, в том числе подключении к сети «Интернет», требуется доказать факт, что именно это лицо использовало данное техническое устройство в период выполнения каких-либо действий в Сети.

В связи с этим необходима иллюстрация технических свойств IP-адреса, его видов и способов установления. Целесообразно отразить особенности установления и соответствия IP-адреса техническому устройству и физическому лицу, а также процессуальные возможности использования сведений о нем в качестве доказательства по расследуемому преступлению.

IP-адрес — четырехбайтовое число, уникально определяющее каждый хост в сети «Интернет», обычно написанное в пунктирно-десятичной системе обозначений с разделением байтов[172].

Понимание структуры IP-адреса как уникального четырехбайтового идентификатора хоста позволяет следователю: верно определять объекты и границы поисково-познавательной деятельности; дифференцировать сведения для осуществления дальнейшей идентификации личности; грамотно выстраивать взаимодействие со специалистами и организаторами распространения информации в сети «Интернет» при подготовке запросов и оценке полученных результатов.

Если посредством технологии происходит выход в сеть «Интернет», то IP-адрес технологии и IP-адрес узла сети взаимодействуют, и появляется адрес того субъекта, который произвел выход в сеть «Интернет»[173]. Например, устройству, подключившемуся к сети «Интернет», был присвоен IP-адрес 192.156.168.35, где первые две группы чисел, разделенные точками, определяют номер сети, а последние две — номер узла (компьютера или иного устройства).

Существуют статические и динамические IP-адреса. Статические IP-адреса являются постоянными, неизменными. Данные адреса назначаются устройству в

---

[172] См.: ГОСТ Р 53632-2009 «Показатели качества услуг доступа в Интернет. Общие требования».

[173] См.: Жарова А. К. Право и информационные конфликты в информационно-телекоммуникационной сфере : монография. М. : Янус-К, 2016.

Сети на постоянной основе согласно договору об оказании услуг связи, в том числе предоставлении доступа к сети «Интернет», заключенному между абонентом и провайдером, и не меняют свое значение с течением времени. Таким образом, при каждом подключении любого устройства к Сети ему присваивается один и тот же IP-адрес.

Следствием этого и выгодным для расследования будет являться то, что все действия с использованием сети «Интернет» производятся в одной географической точке, т.е. с определенного неизменного местоположения. Данное обстоятельство положительным образом влияет на ход расследования и позволяет оптимизировать его сроки.

Динамический IP-адрес, напротив, меняется при каждом подключении устройства к Сети, назначается автоматически и используется в течение ограниченного промежутка времени (до завершения сеанса подключения к сети «Интернет»)[174]. Таким образом, при подключении устройства к Сети ему будет присвоен IP-адрес со значением, скажем, 92.124.163.183, а при последующем подключении того же устройства — IP-адрес с другим значением, например 92.124.163.184, вне зависимости от того, с какого устройства осуществляется подключение. Следствием этого будет являться то, что подключение может производиться с разных географических точек, однако совпадение номера сети в последующих подключениях может свидетельствовать о территориальной близости друг к другу точек доступа.

Более того, в разные промежутки времени динамические IP-адреса устройств могут совпадать, так как при их подключении к сети «Интернет» им присваивается любой свободный от подключения динамический IP-адрес, входящий в диапазон адресов, имеющихся у провайдера, обслуживающего данное подключение.

Следствием этого является то, что совпадение динамических IP-адресов при неоднократных подключениях устройств к сети «Интернет» не дает однозначных оснований полагать, что соответствующие подключения и дальнейшие действия с

[174] См.: Медведева Т. М. Если у налогоплательщика и его контрагента один IP-адрес // Актуальные вопросы бухгалтерского учета и налогообложения. 2017. № 10. С. 63.

использованием Сети осуществлялись одним и тем же человеком или ограниченной следователем группой лиц. Поскольку во всех случаях динамический IP-адрес присваивается каждому подключающемуся к сети «Интернет» устройству в случайном порядке, то велика вероятность, что в разное время доступа к Сети у нескольких устройств совпадут IP-адреса. В связи с этим С. И. Кувычков обращает внимание на то, что чаще всего динамический IP-адрес компьютеру, подключаемому к Сети, назначается провайдером автоматически, а потому при разнице во времени, определяемом часовыми поясами, под данным IP-адресом с интервалом даже в один час могут работать разные пользователи. В судебной практике известны случаи, когда правоохранительные органы, не учитывая указанный момент, изымали компьютерную технику и пытались обвинить людей, не причастных к совершению преступления[175]. В научной литературе и в практической деятельности описываются ситуации, когда выход в сеть «Интернет» осуществляется из одной публичной точки доступа с использованием сети WI-FI, например, в квартире всеми членами семьи или в кафе различными посетителями. Как отмечают В. В. Архипов, В. Б. Наумов, Г. А. Пчелинцев, Я. А. Чирко, при отсутствии дополнительных мер аутентификации, таких как аутентификация с помощью СМС-сообщений, IP-адрес будет в лучшем случае ограничивать группу лиц, которые совершают действия в сети «Интернет»[176]. Тем не менее у следователя будут основания для выдвижения версии относительно возможного круга причастных к совершенному преступлению лиц, которая в дальнейшем будет подлежать проверке.

Впрочем, с течением времени, как мы указывали выше, совершенствуются меры по соблюдению идентификации пользователя, одной из которых является идентификация пользователей сети «Интернет», передачу электронных сообщений которых осуществляет организатор сервиса обмена мгновенными сообщениями

---

[175] См.: Кувычков С. И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 2. С. 76–81.

[176] См.: Архипов В. В., Наумов В. Б., Пчелинцев Г. А., Чирко Я. А. Открытая концепция регулирования Интернета вещей // Информационное право. 2016. № 2. С. 18–25.

(далее — пользователи сервиса обмена мгновенными сообщениями), по абонентскому номеру оператора подвижной радиотелефонной связи в порядке, установленном Правительством Российской Федерации, на основании договора об идентификации, заключенного организатором сервиса обмена мгновенными сообщениями с оператором подвижной радиотелефонной связи, за исключением случаев, предусмотренных Федеральным законом от 29.07.2017 № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона “Об информации, информационных технологиях и о защите информации”». Под сервисами мгновенного обмена сообщениями подразумеваются различные мессенджеры. Не следует исключать того, что в дальнейшем такие требования об идентификации по абонентскому номеру будут распространяться на использование и других ресурсов сети «Интернет».

Следует отметить, что проблема совпадения IP-адресов постепенно находит свое решение в повседневной жизни. Поскольку существуют две версии IP-адресов (в версии IPv4 IP-адрес имеет длину 32 бита (192.158.0.2.), а в версии IPv6 — 128 бит (2001:0db8:85a3:0000:0000:8a2e:0370:7334)), в последнее время происходит внедрение IP-адресов шестой версии в связи с исчерпанием резерва уникальных IP-адресов четвертой версии. Это не случайно, поскольку аудитория пользователей сети «Интернет» стремительно пополняется с каждым годом. Ввиду того, что количество IP-адресов четвертой версии составляет около 4 млрд[177], с целью исключения совпадения IP-адресов происходит внедрение в работу адресации в сети «Интернет» IP-адресов шестой версии, количество которых будет более 340 трлн. В настоящее время одновременно используются обе версии.

Исходя из разделения IP-адресов на статические и динамические, необходимо подчеркнуть, что при использовании статического IP-адреса значительно сужаются рамки доказывания такого обстоятельства, как событие преступления, поскольку в данном случае действия с использованием ресурсов

[177] Сегодня интернет переходит на новый протокол IPv6 [Электронный ресурс] // URL: https://web.archive.org/web/20211127094000/https://ain.ua/2012/06/06/segodnya-internet-perexodit-na-novyj-protokol-ipv6/ (дата обращения: 10.12.2024).

сети «Интернет» осуществляются из одной географической точки. При использовании динамического IP-адреса географический разброс может быть довольно обширен. В то же время как при статическом, так и при динамическом IP-адресах сложность заключается в идентификации конкретного лица с помощью такого IP-адреса, учитывая то, что может быть неограниченный круг лиц, имеющих возможность использовать устройства для подключения к сети «Интернет» с одной точки доступа.

Подключившемуся к сети «Интернет» техническому устройству присваивается IP-адрес, который назначается из числа свободных на данный промежуток времени (не занятых при других подключениях) из диапазона адресов, имеющихся в распоряжении провайдера. В связи с этим Администрация адресного пространства в сети «Интернет» (Internet Assigned Numbers Authority (IANA)), одной из функций которой является управление пространствами IP-адресов, доменов верхнего уровня, должна наделить полномочиями по регистрации провайдеров хостинга региональный интернет-регистратор, а провайдеры хостинга должны пройти регистрацию у регионального интернет-регистратора и получить свой диапазон IP-адресов. Таким образом, через услуги провайдеров хостинга более мелкие провайдеры предоставляют доступ в сеть «Интернет» своим пользователям (клиентам) — физическим и юридическим лицам на основании договора об оказании услуг связи, в частности предоставлении доступа к сети «Интернет».

Исходя из этого, следователю необходимо осуществлять взаимодействие именно с теми провайдерами, которые предоставили доступ в сеть «Интернет» в конкретном регионе по определенному физическому адресу, с целью получения сведений об IP-адресе и в целом о пользователе.

В рамках осуществления такого взаимодействия, обязывающего организаторов распространения информации предоставлять подобного рода сведения уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности России, следователю предлагается выстраивать ход расследования в зависимости от того,

установлен ли IP-адрес или его требуется установить. В случае, когда IP-адрес не установлен, полагаем целесообразным делать это следующими способами:

1) посредством направления запроса в порядке ч. 4 ст. 21 УПК РФ в адрес компании-провайдера, оказывающей услуги доступа к сети «Интернет» по определенному физическому адресу. Первоначально, когда провайдер неизвестен, следует направлять запрос в адрес управляющей организации по месту проживания интересующего лица для определения всех провайдеров, предоставляющих услуги доступа к сети «Интернет» по конкретному адресу. В ответе на такой запрос будут содержаться сведения о наименованиях провайдеров, с которыми был заключен договор о предоставлении доступа к услугам связи, в том числе к сети «Интернет», по адресу, указанному в данном запросе. После этого следует направить запросы по адресам установленных организаций-провайдеров с требованием предоставить информацию о том, оформлен ли договор об оказании услуг связи, в том числе подключении к сети «Интернет», данным провайдером по указанному адресу. Если ответ положительный, то правоохранительным органам должны быть предоставлены следующие сведения:

— полные данные, указанные лицом при заключении договора об оказании интернет-услуг (фамилия, имя, отчество, адрес, телефон, копия паспорта);

— используемые пользователем IP-адреса в определенный промежуток времени (исходя из обстоятельств совершенного деяния);

— адрес местонахождения приемопередающего оборудования, посредством которого осуществлялся выход в Интернет через указанные IP-адреса;

— информация о том, статическими или динамическими являются указанные IP-адреса;

— информация о том, использовались ли специальные программные средства и DNS-серверы с целью модификации истинного IP-адреса (при наличии таких сведений);

— информация об используемом 3G-, 4G-, 5G-модеме (номер сим-карты, MAC-адрес[178]), посредством которого осуществлялся выход в Интернет через указанные IP-адреса[179].

Полученную информацию, отраженную организацией-провайдером в соответствующем документе, следует приобщать в качестве доказательства в порядке ст. 74 УПК РФ как иной документ.

Важно отметить, что запрос организации-провайдеру необходимо направлять вместе с постановлением суда о разрешении получения такой информации, поскольку она содержит сведения, относящиеся к категории персональных данных.

Исходя из этого, можно сказать о том, что полученные следователем в ходе выполнения следственных действий и оперативно-разыскных мероприятий сведения об IP-адресе могут косвенно относиться к определенному или определяемому физическому лицу. Более того, при ответе на запрос от правоохранительных органов провайдер предоставляет информацию об IP-адресе, которая включает в себя персональные данные физического лица.

В ситуации, когда сервер интернет-ресурса располагается вне юрисдикции Российской Федерации, получение сведений о пользователе осуществляется путем направления запроса о правовой помощи в компетентные органы соответствующего иностранного государства в порядке, предусмотренном международными договорами и нормами гл. 53 УПК РФ;

---

[178] MAC-адрес является уникальным идентификатором (например, 64:BC:0C:10:F0:D8), поскольку он уже присвоен или, так сказать, «вшит» в сетевую карту компьютера или маршрутизатора заводом-производителем; диапазон таких адресов он получает в координирующем комитете IEEE Registration Authority — регистрационной администрации Института инженеров электротехники и электроники. При осуществлении устройством подключения к сети «Интернет» провайдером фиксируется MAC-адрес данного устройства, который без совершения целенаправленных действий по его модификации является неизменным. Таким образом, возникает возможность сопоставления MAC-адресов изъятого у лица электронного устройства с теми, которые были зафиксированы при совершении преступлений и установлены сотрудником в рамках расследования уголовного дела.

[179] Сидорова К. С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел. С. 88–92 ; Она же. Криминалистически значимые сведения, получаемые из ресурсов информационно-телекоммуникационной сети «интернет» в ходе расследования преступлений // Современные тенденции развития юридической науки : материалы международной научно-теоретической конференции молодых ученых, посвященной Дню казахстанской науки / под общ. ред. канд. юрид. наук, доцента А. Дарменова. Караганда : Карагандинская академия МВД Республики Казахстан имени Б. Бейсенова, 2022. С. 70–72.

2) посредством направления мотивированного запроса в адрес администрации сайта, на котором зарегистрирован пользователь, интересующий следователя в рамках расследования преступления.

Для осуществления своих потребностей пользователь регистрируется на различных сайтах, указывая свои персональные данные. В результате этого при работе на сайте после регистрации он использует никнеймы/ники/логины, идентификационные номера, адрес электронной почты и др., которые являются его «видимыми» идентификаторами. Получается, что параллельно фиксируется техническая составляющая подключения к сети «Интернет» по конкретному логину / никнейму / идентификационному номеру в виде IP-адресов, по которым получают объем полезной для органов предварительного расследования информации.

После установления сайта, где зарегистрирован интересующий орган расследования пользователь, следует направить запрос в адрес администрации этого сайта с требованием предоставить:

— сведения, которые указывало лицо при регистрации аккаунта на определенном сайте (ФИО, телефон, электронную почту и иную информацию);

— данные об IP-адресе и интенсивности посещения сайта в определенный промежуток времени.

Установив такие сведения, посредством следственных и иных процессуальных действий, оперативно-разыскных мероприятий следует выяснить наименование провайдера, в сети которого зарегистрирован установленный IP-адрес, и его географическое местоположение.

В этих целях в настоящее время существуют специальные интернет-сайты: WHOIS, 2IP, RIPE и др., располагающие информацией в том числе и об IP-адресе. При запросе об IP-адресе или доменном имени на таких сайтах выдается информация о стране, городе, названии провайдера.

Примечательно, что деятельность данных сайтов со стороны государства не контролируется, но из анализа пользовательских соглашений вышеперечисленных сайтов следует, что их функционирование построено в соответствии с

требованиями действующего российского законодательства и направлено на регулирование взаимоотношений между администрацией, пользователями сайта и провайдерами (права, обязанности, пределы ответственности).

Анализ пользовательских соглашений названных сайтов показывает, что в случае неточности, недостоверности, необъективности предоставляемых ими данных, а также отклонений в части качества оказания услуг их администрация ответственности не несет. В связи с этим возникает вопрос относительно степени доверия правоохранительных органов к сведениям, размещаемым на таких сайтах. Соответственно, не следует исключать ситуации, когда сервисами данных сайтов будет предоставлена неточная или неверная информация по определению провайдера, присвоившего конкретный IP-адрес, и его географического местоположения. Практике расследования преступлений известны случаи, когда сведения с вышеперечисленных сайтов приобщались к уголовному делу в качестве вещественных доказательств. Например, согласно приговору Волжского городского суда Волгоградской области от 24.10.2016 по делу № 1-998/2016 по обвинению Чертовских В. Г. в совершении преступления, предусмотренного частью 2 ст. 159 УК РФ, одним из вещественных доказательств по делу послужили сведения с сервера WHOIS, полученные в рамках оперативной проверки[180]. Следует отметить, что данный случай не является единичным, а по результатам опроса сотрудников правоохранительных органов установлено, что сведения с подобных сайтов используются сотрудниками, осведомленными о соответствующих возможностях, в процессе расследования в качестве как ориентирующей, так и доказательственной информации.

Несмотря на возможную неточность сведений, полученных с таких неофициальных сайтов, мы всё же считаем целесообразным использовать подобные ресурсы для изучения IP-адреса, установленного в ходе расследования преступлений. С целью уточнения сведений об IP-адресе и исключения вероятности ошибки возможно проверять один и тот же IP-адрес на нескольких

[180] URL: https://rospravosudie.com/court-volzhskij-gorodskoj-sud-volgogradskaya-oblast-s/act-535499180/ (дата обращения: 11.12.2017).

сайтах. Безусловно, такие сведения могут послужить ориентиром для построения дальнейшей тактики расследования преступлений.

В целях проверки информации об IP-адресе, полученной на одном из указанных сайтов, и использования ее в качестве доказательства по уголовному делу считаем целесообразным направлять в адрес соответствующей организации-провайдера, в диапазоне которой находится необходимый IP-адрес, запросы об установлении факта принадлежности или непринадлежности определенного IP-адреса диапазону IP-адресов, имеющихся у провайдера. Таким образом, полученная с названных сайтов информация либо найдет свое подтверждение, либо будет опровергнута, что побудит следователя проверять данную информацию и путем соответствующего поручения органам, осуществляющим оперативно-разыскную деятельность;

3) посредством направления органу дознания поручения об установлении IP-адреса конкретного соединения (соединений) по обстоятельствам совершенного преступления. Данный способ может реализовываться соответствующими подразделениями с использованием специального программного обеспечения, оперативно-разыскных мероприятий и т.д.;

4) посредством проведения таких следственных действий, как осмотр, в частности, электронных носителей информации, под которыми в данном случае будут пониматься компьютеры, мобильные телефоны, планшеты и др., и их выемка. Безусловно, с целью сохранения всех сведений на соответствующем носителе, а также при невозможности получения доказательственной информации иными способами[181] следует осуществлять его выемку и направлять на экспертизу. Но вместе с тем, если требуется выяснить только сведения об IP-адресах, которые присваивались данному подключению к сети «Интернет», допустимо ограничиться лишь осмотром с участием специалиста.

Перечень действий по установлению IP-адреса не является исчерпывающим. Нами указаны наиболее приемлемые с тактической точки зрения действия

[181] См.: Варданян А. В., Никитина Е. В. Расследование преступлений в сфере высоких технологий и компьютерной информации. М.: Юрлитинформ, 2007.

следователя при расследовании преступления. Вопрос о том, каким способом воспользоваться, оценивается индивидуально, применительно к каждой конкретной ситуации и зависит от обстоятельств совершенного преступления, а также объема имеющейся информации по делу в целом.

Определив IP-адрес, необходимо производить комплекс следственных действий и оперативно-разыскных мероприятий, нацеленных на установление соответствия между IP-адресом, устройством и совершившим преступление физическим лицом. Данный комплекс должен быть направлен на детализацию показаний лиц, имеющих отношение к сетевому подключению (в первую очередь — законного владельца абонентского устройства), проверку таких показаний и формирование на их основе совокупности допустимых доказательств по уголовному делу.

Вместе с тем полагаем необходимым в ходе следственных действий и оперативно-разыскных мероприятий:

— установить точное время доступа устройства, использовавшегося пользователем, к сети «Интернет» (час, минуту, секунду местного времени) в ходе осмотра;

— произвести осмотр журнала лог-файлов с целью подтверждения или опровержения факта соединения с использованием конкретного IP-адреса;

— детально зафиксировать в протоколах следственных действий сведения, которые указывают на соответствующий временной промежуток подключения к сети «Интернет», чтобы максимально сузить круг лиц, имеющих отношение к преступному деянию, в случае совпадения IP-адресов;

— произвести выемку документов, подтверждающих наличие подключения к сети «Интернет» (например, договора об оказании услуг связи, в том числе предоставлении доступа к сети «Интернет»), детально их осмотреть и зафиксировать сведения об IP-адресе, его виде;

— произвести выемку и осмотр устройств, назначить судебную компьютерную экспертизу с целью установления связки IP-адреса с конкретным устройством по его уникальным идентификаторам (IMEI, MAC-адресу);

— изъять и осмотреть записи с камер видеонаблюдения с целью подтверждения или опровержения местонахождения лица в конкретный период времени.

Следует отметить, что, помимо вышеизложенных моментов, при установлении соответствия между IP-адресом и физическим лицом могут иметь место не менее сложные ситуации, связанные с умышленными действиями лица по изменению, маскировке, утаиванию истинного IP-адреса. Преступник, как правило, использует динамический IP-адрес, предоставляемый анонимными прокси-серверами, а также последовательностью анонимных прокси-серверов. Такие злоумышленники применяют АнтиАОН и другие программные средства, маскирующие реальный IP-адрес[182], что тоже требует осуществления соответствующих мероприятий по проверке. А. К. Жарова также отмечает, что разработаны программные технологии, которые позволяют менять IP-адрес (например, создавать динамические, или «невидимые», или нераспознаваемые IP-адреса)[183]. Данные действия со стороны преступников вызывают сложности не только при установлении истинного использовавшегося IP-адреса, но и при сопоставлении неверного IP-адреса с конкретным человеком.

Материалы практики свидетельствуют о том, что в большинстве совершаемых преступлений, связанных с тайным хищением чужого имущества, мошенничествами, где в качестве орудия совершения преступления задействована сеть «Интернет», происходит модификация истинного IP-адреса. Как следует из приговора Кировского районного суда г. Саратова от 26.03.2014 по делу № 1-89/2014, «Ефименко А.В., являясь активным пользователем сети Интернет, знал, что при подключении к сети оператором (провайдером) поставщика услуг присваивается IP-адрес, по которому его можно было бы идентифицировать. …Решил намеренно скрыть свой IP-адрес, присвоенный ему оператором (провайдером) поставщика интернет-услуг. …Имея познания в области ЭВМ,

[182] См.: Кувычков С. И. Указ. соч. С. 77.

[183] См.: Жарова А. К. О соотношении персональных данных с IP адресом. Российский и зарубежный опыт // Вестник УРФО. Безопасность в информационной сфере. 2016. № 1. С. 62.

находясь у себя дома… используя имеющийся в личном пользовании домашний компьютер и вышеуказанные способы подключения к сети Интернет, подключился к сети Интернет, где в поисковой системе “хххх”, нашел список анонимных сокс-серверов, позволяющих скрыть свой IP-адрес, затем изменил настройки подключения компьютера к сети Интернет, в результате IP-адрес своего компьютера изменил на IP-адрес компьютера — №, присвоенного сокс-сервером, и оборудование конечного сервера, с которым в дальнейшем работал Ефименко А.В.[,] воспринимало не IP-адрес компьютера Ефименко А.В., а IP-адрес, присвоенный ему сокс-сервером»[184].

В качестве примера можно привести еще одну ситуацию: как следует из приговора Железнодорожного районного суда г. Улан-Удэ (Республика Бурятия) от 23.10.2025 по делу № 1-529/2025, «деятельность магазина законспирирована, члены данной группы используют технологию виртуальной частной сети VPN, скрывающей действительный IP-адрес, и (или) интернет-браузер TOR (система прокси -серверов, позволяющая создавать анонимное сетевое соединение). Общение с куратором осуществляется в приватном мессенджере “Telegram” с особым способом шифрования, позволяющем проводить анонимную регистрацию, быстро, безопасно обмениваться сообщениями с использованием вымышленных имен-псевдонимов, исключая возможность контроля со стороны правоохранительных органов»[185].

В подобных случаях также считаем необходимым осуществлять дополнительные меры по проверке IP-адреса, связанные с назначением судебной компьютерной экспертизы и других необходимых следственных действий, если имеются сведения относительно того, что производилась модификация истинного IP-адреса. Свидетельством тому является и обновление имеющихся

---

[184] URL: https://kirovsky--sar.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=125612344&delo_id=1540006&new=0&text_number=1 (дата обращения: 10.12.2024).

[185] Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/1RecpDC2GD6W/?regular-txt=%D0%BF%D1%80%D0%BE%D0%BA%D1%81%D0%B8+%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=08.04.2026&regular-workflow_stage=10&regular-area=&regular-court=&regular-judge=&_=1775656933332&snippet_pos=16638#snippet (дата обращения: 08.04.2026).

законодательных актов, и создание новых, направленных на исключение анонимности пользователя в сети «Интернет».

Не менее информативными и позволяющими установить техническое устройство, с помощью которого осуществлялся доступ в сеть «Интернет», а в последующем и определить физическое лицо (решить задачу изобличения и розыска лица) являются «видимые» идентификаторы: доменное имя, сетевое имя, электронная подпись.

Изучению этих идентификаторов посвящены работы многих ученых в различных областях науки[186]. В настоящем исследовании мы не ставим перед собой задачу изложения и развития теоретических концепций данных идентификаторов, поскольку его задачей выступает их изучение с криминалистической точки зрения для эффективного расследования преступлений.

Под доменным именем понимается обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к размещенной в ней информации[187]. Как правило, в качестве наименования домена используется какое-либо краткое словесное обозначение, отождествляемое пользователем с владельцем домена. Это фрагмент наименования или товарного знака для юридических лиц и фамилия или псевдоним для физических лиц. Кроме того, как те, так и другие регистрируют более общие наименования доменов (car.ru, auto.ru), номера своих телефонов (344586.ru) и иные обозначения[188].

---

[186] См.: Азаров М. С. Доменные имена в структуре гражданского и информационного права // Информационное право. 2010. № 2. С. 11–18 ; Балкунова А. С. Роль сетевого имени (никнейма) во взаимодействии субъектов виртуальной коммуникации : дис. … канд. юрид. наук. М., 2012 ; Звягин В. А. Доменное имя — новое средство индивидуализации // Закон и право. 2010. № 9. С. 89–92 ; Соколова Е. А. Конкуренция информации в законодательстве РФ о товарных знаках и правовых нормах РФ о доменных именах // Законы России: опыт, анализ, практика. 2010. № 4. С. 57–61 ; Тагиров З. И. Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики // Вопросы безопасности. 2018. № 4. С. 28–51 ; Трофимов Е. И. Электронная подпись как средство защиты электронных документов от подделки // Педагогическое образование на Алтае. 2014. № 2. С. 446–447 и др.

[187] П. 15 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации».

[188] См.: Ельчанинова Н. Б. Правовое регулирование споров о доменных именах в сети Интернет // Известия ЮФУ. Технические науки. 2006. № 10. С. 206.

Следовательно, доменное имя является средством индивидуализации интернет-сайта, а также «видимым» идентификатором, по которому возможно установить и разыскать лицо, зарегистрировавшее определенное доменное имя.

Изучение такого идентификатора, как доменное имя, позволяет отметить, что для удобства запоминания и восприятия была создана доменная система имен — Domain name system (DNS), использующая в своей работе протокол типа «клиент — сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о преобразовании доменного имени в IP-адрес[189], что позволяет сопоставлять абстрактное символьное имя (site.ru) с конкретным IP-адресом в сети (198.198.68.200)[190]. Как следствие, доменное имя — это абстракция, соответствующая IP-адресу, но представляющая собой символьную комбинацию, в отличие от IP-адреса, который представлен только числовыми символами. Однако ключевое идентификационное отличие доменного имени от IP-адреса в том, что оно уникально.

Необходимо отметить, что регистрация доменного имени в сети «Интернет», правила которой урегулированы координационным центром национального домена Сети (создание имени собственного сайта), существенно отличается от регистрации аккаунта пользователя на каком-либо сайте в сети «Интернет». Несомненно, различаются уровни сложности этих видов регистрации. Так, например, процедура регистрации доменного имени в сети «Интернет» регламентируется правилами регистрации доменных имен в доменах .RU и .РФ, занимает продолжительный промежуток времени, содержит определенные ограничения при регистрации пользователей[191].

Помимо различий в вышеупомянутых процедурах регистрации возможно отметить и сходство, которое состоит в том, что физическое лицо в обоих случаях

---

[189] См.: Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 2-е изд. СПб. : Питер, 2005. С. 515.

[190] См.: Ельчанинова Н. Б. Указ. соч. С. 209.

[191] См.: Першин А. Н., Сидорова К. С. Использование ресурсов информационно-телекоммуникационной сети «Интернет» в розыскной деятельности следователя. С. 323–328.

указывает свои персональные данные. Соответственно, появляется объект — физическое лицо, которое в дальнейшем следует проверять на причастность к регистрации и функционированию того или иного домена. Именно по нему возможно установить персональные данные лица, на которое зарегистрировано доменное имя, поскольку оно может принадлежать не только юридическим лицам и индивидуальным предпринимателям, но и физическим лицам и государственным органам[192]. Об этом также свидетельствуют и данные из приговоров судов Российской Федерации[193].

Анализ правоприменительной практики позволяет констатировать, что установление лица, зарегистрировавшего доменное имя, чаще всего необходимо в случаях, когда на сайте с конкретным доменным именем осуществляется противоправная деятельность.

С целью определения механизма преступления, совершенного с использованием того или иного интернет-сайта, и его документирования необходимо устанавливать, каким образом осуществлялись вышеуказанные действия, и какие лица могут быть к этому причастны. Соответственно, предполагаем, что первоначально необходимо определить владельца доменного имени.

Как представляется, сведения о регистраторе доменного имени, его географическом положении и контактные данные следователи могут устанавливать, используя специальный сайт АО «Региональный сетевой информационный центр» (https://www.nic.ru/). RU-CENTER, созданный на базе отдела регистрации доменов Российского НИИ развития общественных сетей (РосНИИРОС), учрежден первым администратором национального домена RU — РосНИИРОС. После этого оформляется запрос в адрес регистратора (организации),

---

[192] См.: Быстров А. К. Доменное имя и связанные с ним объекты // Современное право. 2014. № 5. С. 59.

[193] Приговор Московского районного суда г. Чебоксары Чувашской Республики от 04.03.2016 по делу № 1-69/2016 в отношении С. Е. Енцова [Электронный ресурс] // URL: https://moskovsky--chv.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=94247245&delo_id=1540006&new=0&text_number=1 (дата обращения: 17.04.2018).

зарегистрировавшего конкретный домен, с требованием передачи правоохранительным органам:

− информации, указанной лицом (организацией) при регистрации домена (контактных данных, адреса электронной почты, паспортных данных или копии паспорта);

— копии договора с лицом (организацией), пользовавшимся доменом;

— сведений о способе оплаты за использование домена с указанием средств платежа (расчетного счета; номера пластиковой карты; платежной системы, абонентского номера), копий платежных документов (при наличии);

— при наличии технической возможности информации об IP-адресах и MAC-адресах устройств, работавших с указанным доменом в определенный промежуток времени;

— иной информации, посредством которой возможно установить лицо, зарегистрировавшее домен.

Полагаем, что перечень обстоятельств, подлежащих выяснению у регистратора (организации), зарегистрировавшего конкретный домен, может расширяться исходя из деталей совершенного преступления. При этом для запроса такой информации в отдельных случаях может потребоваться постановление суда, если ее получение может ограничить или нарушить права человека.

Дальнейшие действия правоохранительных органов будут иметь специфику, определяемую объемом информации, полученной от регистратора того или иного доменного имени.

По установленным персональным данным (фамилии, имени, отчеству, телефону, копии паспорта, электронной почте) необходимо:

— проверить лицо по всем доступным разыскным и криминалистическим учетам в органах внутренних дел по фамилии, имени, отчеству;

— запросить сведения о месте жительства и пребывания лица с полученными установочными данными в Управлении по вопросам миграции МВД России (по субъекту Российской Федерации);

— установить владельца сим-карты с определенным абонентским номером, для чего перейти на официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) сервис проверки номера https://www.nic-t.ru/bdpn/bdpn-proverka-nomera/ ввести абонентский номер, а затем направить запрос соответствующему оператору связи с требованием предоставить определенные сведения: персональные данные лица (организации), на чье имя зарегистрирован конкретный абонентский номер в сети определенного оператора сотовой связи, а именно фамилию, имя, отчество, дату и место рождения, место жительства и (или) регистрации; место регистрации абонентского номера; входящие и исходящие соединения, СМС-сообщения с абонентского номера с указанием установочных данных контрабонентов и их географического местонахождения в момент соединения; географическое местоположение абонентского номера в определенный период времени (с указанием базовых станций); IMEI телефонов, с которыми работала сим-карта в определенный период времени; сведения о подключении абонентского номера к услуге «мобильный банк» с указанием номеров карт банков, к которым она подключена; договор об оказании услуг подвижной радиотелефонной связи, заключенный с пользователем сим-карты с указанным абонентским номером, и данные дилеров (распространителей), заключивших этот договор (название компании, адрес, телефон, фамилию, имя, отчество директора);

— установить владельца электронного почтового ящика, для чего направить запрос по юридическому адресу зарегистрировавшей его организации с требованием предоставить следующие сведения: данные, которые указывало лицо при регистрации электронного почтового ящика (телефон, фамилию, имя, отчество, абонентский номер, паспортные и иные данные); IP-адреса и интенсивность посещения почтового ящика с момента регистрации по настоящее время; иные сведения, которые имеются в отношении данного электронного почтового ящика в указанный промежуток времени.

По установленным IP-адресам, используемым пользователем, целесообразно используя с помощью интернет-ресурсов www.2IP.ru/,

https://www.ripe.net/ определить провайдера сети «Интернет», который обеспечивал соответствующие подключения и выделял такие IP-адреса, и его географическое местоположение. После этого необходимо направить запрос в адрес этого интернет-провайдера с требованием предоставить определенные сведения: полные данные, указанные лицом при заключении договора об оказании услуг связи, в том числе обеспечении доступа к сети «Интернет» (фамилию, имя, отчество, адрес, телефон, копию паспорта и копию договора); вид используемых IP-адресов (статические или динамические); адрес местонахождения приемопередающего оборудования, посредством которого осуществлялся выход в сеть «Интернет» через указанные IP-адреса, используемые в соответствующий промежуток времени; MAC-адреса; информацию об используемом 3G-, 4G-, 5G-модеме (номер сим-карты), посредством которого осуществлялся выход в сеть «Интернет» через такие IP-адреса; иные сведения, которые имеются у провайдера в отношении данного пользователя и подключений, которые им осуществлялись в определенный промежуток времени.

По установленным сведениям о платежных операциях необходимо по номеру интернет-кошелька, на который поступили денежные средства, направить запрос в соответствующую организацию электронной платежной системы, обслуживающую данный счет, с требованием предоставить следующую информацию: персональные данные лица (организации), на чье имя зарегистрирован счет; IP-адреса, под которыми регистрировался счет с момента регистрации по настоящее время; номера терминалов (адреса их установки), при помощи которых осуществлялась регистрация счета; транзакции по счету за определенный период времени; информацию о выводах денежных средств на другие счета и (или) номера банковских карт (расчетных счетов) с указанием номера счета и принадлежности к кредитной организации; иные сведения, которые имеются по данному счету.

Устанавливая сведения о лице, на которое зарегистрировано доменное имя, сталкиваются с ситуацией, когда владелец домена оказывается человеком, не имеющим к нему никакого отношения. Подобная ситуация встречается и при

установлении сведений об IP-адресе, что свидетельствует о необходимости проводить «традиционные» следственные действия[194], результаты которых с точностью будут указывать на того или иного человека. К числу таких следственных действий можно отнести: допрос с применением тактического приема — детализации показаний; осмотр технического устройства; назначение судебной компьютерно-технической экспертизы.

Не менее эффективным в расследовании преступлений является исследование такого идентификатора пользователя сети «Интернет», как сетевое имя. Исследования в области лингвистики позволяют определить множество его синонимов: «никнейм», «ник», «интернет-прозвище», «псевдоним», «компьютерное имя», «имя пользователя», «неофициальное личное имя» и т.д.[195]

Следует отметить, что сферы существования и функционирования сетевых имен различны:

1) коммуникативная сфера, в которую включены все социальные сети, интернет-форумы, блогосфера и чаты;

2) культурно-развлекательная сфера, т.е. игровые порталы, сайты о литературе, культуре, кино, музыке, онлайн-казино и др. (например, никнеймы для пользователей-рецензентов на популярном сайте kinopoisk.ru);

3) масс-медийная сфера Интернета, охватывающая новостные сайты, электронные журналы, газеты;

4) научная сфера, которая охватывает интернет-ресурсы и порталы, ставящие своей целью интеграцию, популяризацию и систематизацию научно-технических знаний;

---

[194] См.: Быков В. М., Макаров Н. И. О регламентации следственных действий // Российская юстиция. 1998. № 2. С. 22.

[195] См.: Якунина М. Л. Особенность интернет-дискурса: никнейм // Филологические науки. Вопросы теории и практики. 2013. № 3-2. С. 218–221 ; Пшегорская Ю. В. Типология молодежных сетевых имен, функционирующих в современном русскоязычном сегменте интернета // Филологические науки. Вопросы теории и практики. 2014. № 1-1. С. 150–154 ; Ляховская А. А. Ник: специфика, графическое оформление и функции // Вестник Полоцкого государственного университета. Серия А, Гуманитарные науки. 2010. № 7. С. 154–161 ; Рянская Э. М., Балкунова А. С. Сетевое имя (никнейм) как языковой знак // Вестник Нижневартовского государственного гуманитарного университета. 2011. № 4. С. 72–76 и др.

5) сфера краудсорсинга — интернет-ресурсов, решающих общественно значимые задачи при помощи неопределенного круга добровольцев (например, для регистрации на сайте Википедии необходимо ввести никнейм)[196].

Для следователя большое значение в процессе расследования будет иметь прежде всего коммуникативная сфера. Это обусловлено тем, что регистрация на интернет-ресурсах в виде сайтов социальных сетей, чатов, форумов не представляет существенных сложностей. Потому вызывает интерес изучение сетевого имени пользователя с целью установления его значения и физического лица, зарегистрированного под ним, и проверки его причастности к преступлению. В связи с этим Е. С. Поликарпов, С. Л. Анисимов справедливо указывают, что использование «сетевого имени — никнейма» в связи со своей зависимостью от персональной (личной) информации о пользователе и алгоритмами большинства сервисов Сети позволят идентифицировать пользователя[197], т.е. физическое лицо.

Несмотря на то что сетевое имя (никнейм) является объектом активного научного интереса со стороны лингвистов и существует немало исследований в данной области[198], оно представляет интерес для изучения с криминалистической точки зрения.

Как отмечают Э. М. Рянская, А. С. Балкунова, возникновение сетевых имен (никнеймов) связано с новым видом коммуникации и имеет целью не столько скрыть реальную информацию о себе, сколько позиционировать себя в виртуальном мире, подчеркнув личностные черты или создав определенный образ, чаще всего придуманный[199]. Из этого следует, что в ходе осуществления противоправной деятельности преступники с целью маскировки своей личности

---

[196] См.: Авчиева Д. Т. Системные связи термина «никнейм» // Гуманитарные науки и образование. 2015. № 4. С. 104.

[197] Поликарпов Е. С., Анисимов С. Л. О некоторых аспектах идентификации пользователя сети интернет // Охрана, безопасность, связь. 2017. № 1-2. С. 109.

[198] См.: Аникина Т. В. Имя собственное в интернет-коммуникации // Известия Уральского государственного университета. Серия 1. Проблемы образования, науки и культуры. 2010. № 2. С. 71–76 ; Асмус Н. Г. Лингвистические особенности виртуального коммуникативного пространства : дис. … канд. филол. наук. Челябинск, 2005 ; Балкунова А. С. Ценностные составляющие концепта «Я» языковой личности интернет-пространства // Ценности и смыслы. 2012. № 1. С. 99–105 ; Якунина М. Л. Особенность интернет-дискурса: никнейм // Филологические науки. Вопросы теории и практики. 2013. № 3-2. С. 218–221 и др.

[199] См.: Рянская Э. М., Балкунова А. С. Сетевое имя (никнейм) как языковой знак // Вестник Нижневартовского государственного гуманитарного университета. 2011. № 4. С. 72.

путем анонимизации и сокрытия следов пребывания в сети «Интернет» используют такие сетевые имена, которые первоначально не несут в себе какой-либо значимой информации для расследования. Например, увидев на каком-либо сайте пользователей с сетевыми именами вроде «Кэп», «Kurator», «shkiper», «Gygaga Gygaga»[200], «мартын коробкин»[201] не предполагается возможным сделать вывод о том, с чем связан выбор подобного сетевого имени, без использования специальных знаний.

В связи с этим следователю целесообразно производить следственные и иные процессуальные действия, направленные на установление сведений о сетевом имени пользователя — физического лица.

Такие сведения могут содержать:

— данные, отражающие значение того или иного никнейма;

— данные, которые лицо указывало при регистрации аккаунта с определенным никнеймом (фамилию, имя, номер телефона);

— данные, отражающие технологическое взаимодействие пользователя с используемым никнеймом с интернет-сайтом, на котором он зарегистрировался (IP-адреса, MAC-адреса, количество сессий пребывания пользователя на сайте, точное время входа на сайт и выхода с него).

Одним из способов установления сведений, отражающих значение сетевого имени, является проведение лингвистической экспертизы, особенности которой применительно к исследованию никнеймов изложены в отдельных работах[202].

В рамках семантического исследования эксперту могут быть поставлены следующие вопросы:

---

[200] Приговор Якутского городского суда Республики Саха (Якутия) от 19.01.2018 по делу № 1-41/2018 [Электронный ресурс] // URL: https://jakutsky--jak.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=2325110&delo_id=1540006&new=0&text_number=1 (дата обращения: 25.02.2023).

[201] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа — Югры от 30.06.2015 по делу № 1-777/2015 [Электронный ресурс] // URL: https://rospravosudie.com/court-nizhnevartovskij-gorodskoj-sud-xanty-mansijskij-avtonomnyj-okrug-s/act-495724621/ (дата обращения: 25.02.2023).

[202] См.: Соколова Т. П. Нейминговая экспертиза: генезис, проблемы, перспективы // Вестник Университета имени О.Е. Кутафина. 2014. № 3. С. 148 ; Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М. : Проспект, 2012. С. 342 ; Лингвистическая экспертиза [Электронный ресурс] // URL: http://www.sudexpert.ru/possib/lingv.php#_ftn1 (дата обращения: 11.03.2024).

— какие значения имеет сетевое имя;

— имеется ли в никнейме указание на имя, фамилию, отчество лица;

— содержатся ли в сетевом имени какие-либо данные, указывающие на биографию лица (пол, возраст, образование, место рождения, место жительства, пребывания);

— содержатся ли в сетевом имени сведения, свидетельствующие о личных деловых и моральных качествах;

— имеются ли в сетевом имени сведения, указывающие на нарушение уголовно-правовых норм, действующего законодательства, общепринятых моральных норм и принципов?

По результатам интервьюирования экспертов-лингвистов было выявлено, что случаи назначения лингвистической экспертизы по никнейму крайне редки. Однако такие сведения могут пополнить информацию о личности искомого физического лица, зарегистрированного под определенным никнеймом, в условиях дефицита сведений о нем; в дальнейшем их также можно сопоставить с конкретным физическим лицом.

Полагаем, что с целью соблюдения разумных сроков уголовного судопроизводства, экономичного расходования сил и средств правоохранительных органов следователю целесообразно самостоятельно устанавливать значение сетевого имени путем изучения общедоступных источников, в том числе словарей. При возникающих трудностях, связанных с тем, что для понимания того или иного сетевого имени порой необходимы более углубленные знания истории, географии, литературы, современной массовой культуры, имен известных и публичных личностей, считаем полезным производить допрос эксперта-лингвиста. Если же в распоряжении следователя имеются переписка пользователя с другими пользователями, контент сайта, где она осуществлялась, то в этих случаях лингвистическую экспертизу следует проводить вместе с компьютерно-технической и автороведческой для определения принадлежности конкретных высказываний определенному пользователю, а в целом для установления отдельных частей механизма преступления.

Следует отметить, что сетевое имя пользователя, являясь «видимым» идентификатором пользователя сети «Интернет», несет в себе массив криминалистически значимых сведений, отражающихся на интернет-сайте и хранящихся у администратора. Такие сведения могут содержать:

— данные, которые указывало лицо при регистрации аккаунта с определенным сетевым именем (абонентский номер, фамилию, имя, отчество, иные имеющиеся данные);

— историю изменения данных пользователя: смену имени пользователя, номера мобильного телефона;

— IP-адреса и интенсивность посещения интернет-сайта пользователем с таким сетевым именем с момента регистрации по настоящее время;

— MAC-адрес либо IMEI пользователя и иные характеристики оконечного оборудования пользователя;

— сведения о платежных операциях, проведенных пользователем с данным сетевым именем в интересующий момент времени;

— электронную переписку пользователя;

— иные сведения об указанном пользователе.

К числу «видимых» идентификаторов пользователя возможно отнести и электронную подпись. Понятие электронной подписи дает закон[203].

Различают простую электронную подпись и усиленную электронную подпись (квалифицированную и неквалифицированную) и неразрывную с ней машиночитаемую доверенность. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Усиленная электронная подпись дополняется еще одним значением, которое позволяет не только определить лицо, подписавшее документ, но и обнаружить факт внесения изменений в электронный документ после его

[203] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

подписания. Машиночитаемая доверенность — это цифровой документ, который подтверждает право субъекта пользоваться подписью от имени кампании.

Научные исследования в области специфики и функционирования электронной подписи показывают высокую эффективность ее использования при проведении операций, связанных с передачей документов посредством информационно-телекоммуникационных сетей, т.е. электронном документообороте[204].

Помимо использования различных видов электронной подписи в ходе электронного документооборота, ее широкое применение имеет место и в ходе использования различных ресурсов сети «Интернет». Применение простой электронной подписи решает задачи по подтверждению важных операций или действий пользователя: позволяет подписывать и отправлять сообщения, получать государственные и муниципальные услуги. При этом для осуществления самой процедуры подписания используются технологии пары «логин — пароль», СМС-коды.

Учитывая изложенное, можно сделать вывод о том, что электронная подпись является важным инструментом для выполнения различных операций, связанных не только с электронным документооборотом, но и с действиями, осуществляемыми с использованием сети «Интернет» путем электронной идентификации. Механизм ее использования заключается в следующем. Изначально происходит идентификация: определенный код подтверждает, что конкретный человек осуществил доступ в аккаунт, после чего осуществляется

[204] См.: Вехов В. Б. «Электронная криминалистика»: понятие и система // Криминалистика: актуальные вопросы теории и практики : сборник трудов участников Международной научно-практической конференции. Ростов н/Д. : Ростовский юридический институт МВД России, 2017. С. 40–46 ; Галяутдинов Р. Р. Документы, зафиксированные в электронном виде: особенности процессуальной и криминалистической оценки // Тенденции развития науки и образования. 2023. № 96-5. С. 62–64 ; Дёмин К. Е. О перспективах исследования электронных документов как объектов судебной экспертизы // Вестник экономической безопасности. 2016. № 4. С. 33–37 ; Он же. Электронные документы как носители // Совершенствование деятельности органов предварительного расследования и экспертно-криминалистических подразделений на современном этапе развития России : сборник научных статей. Ставрополь : Секвойя, 2018. С. 59–64 ; Шаповалова Г. М. Электронные документы в уголовном судопроизводстве и криминалистике // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2015. № 12-4. С. 199–202 и др.

подтверждение этого действия: код, присланный, например, на телефон, подтверждает, что пользователь готов совершить вход в аккаунт.

Полагаем, что, установив посредством идентификаторов сведения о пользователе, с целью их проверки, дальнейшего розыска[205] и изобличения лица целесообразно использовать сведения из официальных интернет-ресурсов.

Действующие нормативные правовые акты обязывают различные государственные органы, органы местного самоуправления размещать доступную информацию в сети «Интернет» (например, Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»). Кроме того, согласно Инструкции по эксплуатации аппаратно-программного комплекса «Официальный интернет-сайт МВД России», утвержденной приказом МВД России от 14.01.2013 № 15 «О вводе в эксплуатацию аппаратно-программного комплекса “Официальный интернет-сайт МВД России”», одной из основных задач данного комплекса является публикация информации о разыскиваемых МВД лицах[206].

С целью осуществления поиска на таких ресурсах следователю необходим более полный и точный перечень сведений о лице[207]:

— фамилия, имя, отчество;

— дата рождения;

— место рождения;

— данные документа, удостоверяющего личность (например, серия, номер, дата выдачи паспорта, орган, где он выдавался);

---

[205] См. подробно: Першин А. Н., Сидорова К. С. Использование ресурсов информационно-телекоммуникационной сети «Интернет» в розыскной деятельности следователя. С. 320–325 ; Мазунин Я. М., Сидорова К. С. Розыскная деятельность следователя в информационно-телекоммуникационной сети «Интернет» // Актуальные проблемы правоприменительной деятельности органов внутренних дел : сборник научных трудов. Омск : Омская академия Министерства внутренних дел Российской Федерации, 2019. Т. 4. С. 186–212.

[206] Существуют нормативные акты и иных государственных органов, регулирующие размещение информации в сети «Интернет» (см.: приказ ФНС России от 24.12.2013 № ММВ-7-6/635@ «Об официальном Интернет-сайте Федеральной налоговой службы» ; приказ ФССП России о 14.11.2017 № 541 «Об официальном интернет-сайте Федеральной службы судебных приставов» и др.). Информация о деятельности судов, размещаемая в сети «Интернет», регламентируется Федеральным законом от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

[207] Перечень необходимых данных расширяется в связи с тем, что объектом розыска выступает не только физическое лицо, род его деятельности, но и транспортное средство. Кроме этого, на упомянутых ресурсах отыскать подобного рода сведения возможно только при наличии у следователя точных установочных данных лица.

— идентификационный номер налогоплательщика (ИНН);

— страховой номер индивидуального лицевого счета (СНИЛС);

— данные водительского удостоверения, идентификационный номер транспортного средства (VIN), государственный регистрационный знак, свидетельство о регистрации транспортного средства.

Наиболее востребованными и информативными интернет-ресурсами органов государственной власти с целью поиска и проверки вышеуказанных сведений являются следующие.

1. Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)» (https:// https://www.gosuslugi.ru/).

В результате работы с данным интернет-ресурсом можно получить следующие сведения:

— установить, входит ли паспорт гражданина Российской Федерации в список недействительных российских паспортов, с помощью онлайн-сервиса по вопросам миграции. Посетив этот ресурс, представляется возможным осуществить загрузку файла и проверить данные того или иного паспорта по списку недействительных;

— проверить соответствие информации о номере основного документа, удостоверяющего личность гражданина Российской Федерации на ее территории (внутреннего паспорта), и информации об адресе регистрации по месту пребывания или по месту жительства владельца такого документа путем ввода паспортных данных.

2. Официальный сайт Федеральной налоговой службы (https://egrul.nalog.ru/)

С его помощью можно определить:

— ИНН гражданина;

— ОГРНИП[208] и дату его присвоения;

[208] Расшифруем номер ОГРН, который состоит из 15 цифр, например 309547531400056. Первая цифра может принимать значения 3 и 4. Это признак отнесения государственного регистрационного номера записи: 3 означает, что знак относится к основному государственному регистрационному номеру записи о государственной регистрации индивидуального предпринимателя (ОГРНИП); 4 — к иному государственному регистрационному номеру записи.

— наличие статуса предпринимателя у разыскиваемого лица;

— дату внесения записи о прекращении деятельности ИП;

— налоговую инспекцию, регистрировавшую ИП;

— виды деятельности по ОКВЭД (чем занимается ИП);

— серию, номер и дату свидетельства о государственной регистрации юридического лица.

3. Официальные сайты судебных органов

В результате работы с данными ресурсами возможно установить:

— вид судопроизводства, в котором участвовал гражданин (уголовное, арбитражное, гражданское или административное);

— статус участника судопроизводства (потерпевший, подсудимый, свидетель, истец, ответчик, представитель);

— признан ли гражданин банкротом или находится в стадии банкротства.

4. Официальный сайт Федеральной службы судебных приставов (http://fssprus.ru/iss/ip/)

Указанный ресурс позволяет получить следующую информацию:

— ФИО, дату, место рождения должника;

— номер и дату возбуждения исполнительного производства;

— реквизиты исполнительного документа;

— сумму задолженности;

— наименование и адрес отдела судебных приставов;

— ФИО пристава и его телефон.

5. Официальные сайты по учету лиц, находящихся в розыске

— вкладка «Внимание, розыск!» Министерства внутренних дел Российской Федерации (https://мвд.рф) («Деятельность» → «Все сервисы» → «Внимание, розыск!»);

---

Вторая и третья цифры указывают на год внесения записи в государственный реестр, четвертая и пятая обозначают код субъекта РФ, а цифры 6–14 — это номер записи, внесенной в государственный реестр в течение года. Последняя цифра выполняет контрольную функцию, т.е. предназначена для проверки.

— «Лица, находящиеся в розыске по подозрению в совершении преступлений» Федеральной службы судебных приставов (http://fssprus.ru/iss/suspect_info/).

ВС помощью этих сайтов можно выяснить:

— дату и место рождения подозреваемого;

— наименование органа, инициировавшего розыск;

— статью УК РФ, по которой возбуждено уголовное дело.

В настоящее время ведется работа по размещению ориентировок по розыску наиболее опасных преступников на сайте Министерства внутренних дел РФ. Кроме того, на официальных сайтах управлений МВД России по субъектам Российской Федерации тоже имеется такая вкладка. Помимо этого, на указанных сайтах имеются и вкладки под названием «МВД в социальных сетях», где размещены ссылки на официальные ресурсы МВД России на сайтах социальных сетей. Как показывает практика, у населения популярность и востребованность социальных сетей значительно выше, нежели официальных сайтов органов государственной власти.

6. Официальный сайт Госавтоинспекции (в зависимости от региона, в данном случае — Омская область) (https://гибдд.рф/check/)[209]

Этот ресурс позволяет установить следующую информацию:

— о водителе (проверка факта выдачи водительского удостоверения и наличия данных о лишении права управления: https://гибдд.рф/check/driver#+);

— об автомашине (основные сведения о транспортном средстве и периодах его регистрации в Госавтоинспекции за различными собственниками, сведения о дорожно-транспортных происшествиях: https://гибдд.рф/check/auto);

— о штрафах (сведения о неуплаченных штрафах за правонарушения в области дорожного движения: https://гибдд.рф/check/fines).

Итак, мы рассмотрели наиболее востребованные и информативные интернет-ресурсы органов государственной власти, при работе с которыми появляется

[209] Регион выбирается самостоятельно на сайте.

возможность получить дополнительные сведения о лице и установить его местонахождение. Кроме этого, для повышения эффективности розыска лица или иного объекта следователю необходимо прибегать к размещению разыскных ориентировок, объявлений в группах социальных сетей наряду с официальными сайтами органов государственной власти.

После получения определенного массива информации о разыскиваемом лице или ином объекте возникает вопрос об оформлении соответствующих результатов. Единого установленного законом способа фиксации сведений, полученных из интернет-ресурсов, не установлено, поэтому предлагаем предусмотреть несколько вариантов[210].

В зависимости от производимого следователем действия, направленного на поиск сведений об интересующем лице, указанные результаты могут быть оформлены как в виде протоколов следственных действий, так и в виде справок о проделанной работе по делу. В случае если интерес представляет конкретная веб-страница на каком-либо ресурсе в сети «Интернет», имеется возможность отразить полученную информацию в протоколе ее осмотра. Такой осмотр возможен в рамках возбужденного уголовного дела до его направления в суд. По приостановленному уголовному делу работу с ресурсами в сети «Интернет» целесообразно оформлять справкой. К ней приобщаются приложения, содержащие информацию из названных ресурсов в виде твердых копий электронных файлов, которые включают скриншоты значимых для розыска сведений, сделанные с помощью функции PrintScreen.

Помимо общих данных, которые необходимо отразить в протоколе и справке, следует дополнительно указать:

— дату и время осуществления поиска сведений об интересующем лице или ином объекте на ресурсах сети «Интернет» согласно часовому поясу, в котором производился такой поиск;

---

[210] См., например: Себякин А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации : автореф. дис. … канд. юрид. наук. М., 2021.

— характеристики используемого ЭВМ, тип и версию браузера, параметры интернет-соединения, а также сведения о сетевом адресе (IP-адрес, данные сервиса WHOIS при необходимости);

— физическое место (адрес), откуда осуществлялся поиск;

— результаты проверки доступности осматриваемой интернет-страницы или интернет-сайта (каждая значимая страница фиксируется с указанием ее полного адреса в строке браузера);

— трассировку пути до интернет-страницы (или интернет-сайта);

— описание визуального отображения страницы (текста, заголовков, медиафайлов при их наличии, даты и времени публикации, если они указаны на соответствующем ресурсе)[211];

— программы для снимка экрана (создания скриншотов), записи видеопотока или специализированное криминалистическое программное обеспечение. Здесь следует отметить, что такое программное обеспечение должно быть лицензированным, а средства измерений, применяемые при осуществлении судебно-экспертной деятельности, должны поверяться только аккредитованными в установленном порядке в области обеспечения единства измерений государственными региональными центрами метрологии согласно постановлению Правительства РФ от 20.04.2010 № 250.

Важно отметить, что перечень сведений, отражаемых в соответствующем документе, будет зависеть от обстоятельств дела в целом и объекта искомой информации (так, в нем могут фиксироваться данные об аккаунте разыскиваемого лица, о похищенном объекте на сайте онлайн-продажи имущества или о распространении с определенного аккаунта призывов к осуществлению экстремистской деятельности). Возникают ситуации, когда нет необходимости фиксировать документально сведения, найденные на ресурсах сети «Интернет», поскольку они представляют собой всевозможную ориентирующую информацию

[211] См. подробнее об этом: Фокин А. Д. Принципы и тактика проведения следственного осмотра интернет-ресурса при расследовании дистанционного мошенничества в сфере недвижимости // Российский следователь. 2025. № 3. С. 2–7.

как об интересующей следователя личности, так и о других аспектах совершенного преступления: указание конкретных ресурсов, которые изучил следователь, в виде ссылки на сайт (например, https://vk.com/, https://ok.ru/); параметры, по которым осуществлялся поиск (фамилию, имя, город рождения, ID и др.); адрес учетной записи найденного лица в виде ссылки (https://vk.com/id20200562); сведения, приведенные в личном аккаунте пользователя в форме открытых данных; время последней активности пользователя на сайте и вид устройства, с которого осуществлялся вход (мобильный телефон / персональный компьютер); результат изучения контактов пользователя, личного контента.

Кроме того, как было отмечено выше, с целью получения более подробных данных об аккаунте пользователя, доменном имени, администраторе сайта и других идентификаторах необходимо направлять запросы в адрес организации, их зарегистрировавшей. В связи с этим возникает вопрос о том, какие сведения из интернет-ресурсов фиксировать в запросе для получения полной информации по ним, чтобы не раскрыть в то же время следственную тайну. Рекомендуется указывать следующее:

— факт наличия возбужденного уголовного дела (номер, статью УК РФ);

— сведения о каком-либо идентификаторе пользователя в сети «Интернет» (речь идет о пользователе — физическом лице, причастном к совершению преступления; возможные идентификаторы: фамилия, имя, ID, доменное имя, IP-адрес, никнейм/логин);

— перечень сведений, которые необходимо получить;

— срок направления ответа на запрос и адрес;

— разъяснение ч. 4 ст. 21 УПК РФ, а также ответственности по ст. 17.7 Кодекса РФ об административных правонарушениях;

— приложения (например, постановление суда);

— данные следователя, направляющего запрос (должность, звание, ФИО, контактный телефон).

В ст. 164.1 УПК РФ регламентированы особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий. К числу основных правил относятся:

— специальный субъектный состав: устанавливается обязательность участия специалиста в процессе изъятия электронных носителей и копирования информации. Это минимизирует риск случайного уничтожения или модификации данных вследствие некомпетентных действий следственных органов;

— приоритет копирования информации с электронного носителя; сам материальный носитель (сервер, компьютер, смартфон) изъятию не подлежит и остается у владельца;

— копирование данных должно осуществляться на сертифицированные или надлежащим образом подготовленные носители, исключающие подмену информации. Процесс фиксации должен позволять в дальнейшем подтвердить неизменность скопированных данных (в том числе через механизмы хеширования);

— гарантируется право обладателя информации на получение копии изымаемых данных непосредственно в ходе следственного действия (за исключением случаев, когда это может объективно воспрепятствовать расследованию);

— процессуальное оформление и упаковка: устанавливаются требования к физической сохранности объектов: изъятые носители должны быть упакованы и опечатаны способом, исключающим несанкционированный доступ к содержимому без нарушения целостности упаковки.

## Выводы по второй главе

1. Использование сети «Интернет» как источника криминалистически значимой информации в целях установления события (или его отдельных

элементов) преступления или неизвестных эпизодов преступной деятельности возможно в двух направлениях:

— для определения латентного (зачастую совершаемого с использованием сети «Интернет») посягательства (или его эпизодов/элементов);

— для получения дополнительной криминалистически значимой информации по очевидным преступлениям.

2. В первом направлении обращение к Сети необходимо, как правило, оперативным путем с привлечением специалистов для анализа «Даркнета» и зашифрованных мессенджеров. Акцент следует делать на ключевых субъектах: администраторе сайта; лице, размещающем противоправный контент, и потребителе (заказчике) этого контента. Здесь необходимо также выделить два вектора оперативной и процессуальной работы: 1) от сайта или 2) от потребителя (заказчика).

По первому вектору предлагается в рамках оперативного эксперимента создание копий известных криминальных сайтов либо самостоятельных сайтов — торговых площадок для реализации криминальных товаров и услуг — с дальнейшим отслеживанием заказа и доставки или внедрением компьютерного червя при нематериальном информационном заказе в рамках контролируемой поставки.

По второму вектору при поиске от потребителя (заказчика) рекомендуется использовать информацию провайдера о подключении к входной ноде, сопоставляя время выхода в «Даркнет», подключения к входной ноде и появления определенного преступного результата.

Второе направление, связанное с получением криминалистически значимой информации по очевидным преступлениям, представляет интерес в плане поиска данных, размещаемых на новостных сайтах, популярных развлекательных порталах, стриминговых сервисах и в мессенджерах.

3. Под идентификатором пользователя сети «Интернет» понимается присваиваемая сетевому подключению или задаваемая пользователем уникальная комбинация символов, позволяющая в процессе раскрытия и расследования

преступлений выделять конкретное лицо или оконечное оборудование из неопределенного круга, устанавливать устойчивую связь между виртуальным образом и реальным субъектом, а также документально фиксировать факты присутствия и выполнения отдельных операций в информационно-телекоммуникационной сети «Интернет».

4. Руководствуясь определением идентификатора пользователя, спецификой функционирования, считаем возможным разделить перечисленные идентификаторы — IP-адрес, никнейм/логин, доменное имя — на две группы:

— «видимые» идентификаторы — доменное имя, сетевое имя пользователя, простая электронная подпись;

— «невидимые» идентификаторы — IP-адрес.

5. С целью идентификации конкретного лица в сложной цепочке («физическое лицо → техническое оборудование → подключение к сети “Интернет” → результат действий на определенном ресурсе сети “Интернет” — правомерное или противоправное деяние») необходимо произвести комплекс технических, организационных и тактических мер путем осуществления следственных действий и оперативно-разыскных мероприятий.

6. Для успешного установления соответствия между IP-адресом, устройством и совершившим преступление физическим лицом представляется необходимым проведение комплекса следственных действий и оперативно-разыскных мероприятий. Данный комплекс должен быть направлен на детализацию показаний лиц, имеющих отношение к сетевому подключению (в первую очередь законного владельца абонентского устройства), проверку таких показаний и формирование на их основе совокупности допустимых доказательств по уголовному делу.

7. Вместе с тем полагаем необходимым в ходе следственных действий и оперативно-разыскных мероприятий:

— установить точное время доступа устройства, использовавшегося пользователем, к сети «Интернет» (час, минуту, секунду местного времени) в ходе осмотра;

— произвести осмотр журнала лог-файлов с целью подтверждения или опровержения факта соединения с использованием конкретного IP-адреса;

— детально зафиксировать в протоколах следственных действий сведения, которые указывают на соответствующий временной промежуток подключения к сети «Интернет», чтобы максимально сузить круг лиц, имеющих отношение к преступному деянию, в случае совпадения IP-адресов;

— произвести выемку документов, подтверждающих наличие подключения к сети «Интернет» (например, договора об оказании услуг связи, в том числе предоставлении доступа к сети «Интернет»), детально их осмотреть и зафиксировать сведения об IP-адресе, его виде;

— произвести выемку и осмотр устройств, назначить судебную компьютерную экспертизу с целью установления связки IP-адреса с конкретным устройством по его уникальным идентификаторам (IMEI, MAC-адресу);

— изъять и осмотреть записи с камер видеонаблюдения с целью подтверждения или опровержения местонахождения лица в конкретный период времени.

8. Изучение таких «видимых» идентификаторов пользователя, как доменное имя, сетевое имя пользователя, электронная подпись, при расследовании преступления позволяет определить техническое устройство, с которого осуществлялся доступ в сеть «Интернет» с данными идентификаторами, а также физическое лицо, которое могло его использовать.

# ГЛАВА III. ТАКТИКО-ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ» ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

## § 1. Особенности использования сети «Интернет» при производстве невербальных следственных действий

Тактико-криминалистические рекомендации по производству следственных действий рассматриваются в многочисленных работах, посвященных вопросам расследования преступлений, так или иначе связанных с использованием сети «Интернет»[212]. Однако акцент на тактических особенностях ее использования при производстве невербальных следственных действий в этих трудах делается с позиций анализа следовой картины: авторы указывают на характерные следы преступной деятельности в Сети и описывают процессуальные и тактические особенности их обнаружения, фиксации, изъятия и изучения. За рамками такого подхода остается потенциал сети «Интернет» как высокоэффективного тактического инструментария, обеспечивающего оптимизацию подготовки и проведения следственных действий.

В современных условиях значение и роль ресурсов сети «Интернет» при расследовании преступлений сложно переоценить. Следует констатировать, что эта роль давно не ограничена использованием Сети при расследовании преступлений в сфере компьютерной информации (гл. 28 УК РФ). Проведенное обобщение следственной практики свидетельствует, что в 12 % случаев сеть «Интернет» выступала в качестве объекта преступного посягательства; в 32 % — использовалась в качестве элемента в механизме таких преступлений, как мошенничество, кража, незаконный оборот наркотических средств, психотропных

[212] См., например: Поляков В. В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук. Омск, 2008 ; Колычева А. Н. Указ. соч. ; Бахтеев Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : дис. … д-ра юрид. наук. Екатеринбург, 2022, и др.

средств или их аналогов. При расследовании данных преступлений в большинстве случаев (56 %) сеть «Интернет» служила источником криминалистически значимой информации о социальных связях причастных к преступлению лиц, их передвижениях и иных обстоятельствах, имеющих значение для уголовного дела.

Данная статистическая закономерность обусловливает специфику тактики реализации невербальных следственных действий, проводимых с использованием сети «Интернет». Последнее, на наш взгляд, сводится к решению следующих тактических задач:

1) поисково-познавательные;

2) обеспечительные.

Как показали результаты исследования, в 75 % случаев поисково-познавательные задачи реализуются с целью использования сети «Интернет» для отыскания, фиксации и получения криминалистически значимой информации, которая за счет процессуальной формы проводимого следственного действия преобразуется в доказательственную (естественно, с учетом соответствия критериям относимости и допустимости).

Получены результаты, указывающие на то, что к наиболее частым невербальным следственным действиям, в рамках которых реализуются поисково-познавательные задачи с использованием сети «Интернет», относятся:

— осмотр места происшествия и технических устройств (69 %);

— получение информации о соединениях между абонентами и (или) абонентскими устройствами (42 %);

— обыск, выемка (38 %);

— контроль и запись переговоров (12 %);

— наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (5 %).

Ключевой проблемой реализации невербальных следственных действий, связанных с решением поисково-познавательных задач в сети «Интернет», как показали результаты настоящего исследования, является правильное применение оптимальной уголовно-процессуальной формы получения доказательств.

Данный вывод подтверждается исследованиями различных авторов. Так, по мнению С. В. Пропастина, у следователей при работе с криминалистически значимой информацией в сети «Интернет» существует проблема выбора между осмотром, обыском и компьютерной экспертизой[213]. Это осложняет принятие следователем оптимальных тактических и процессуальных решений о проведении конкретного следственного действия. Отчасти это связано с тем, что закон позволяет получить доступ к сведениям из ресурсов сети «Интернет» разными способами. В результате возникают так называемая конкуренция норм и вариативность в определении наиболее эффективного процессуального порядка получения доказательства.

В частности, в работах В. В. Полякова обращается внимание на проблему разграничения осмотра места происшествия, средств компьютерной техники и электронных документов. Данная сложность связана с пограничным характером осмотра по отношению к обыску и экспертизе[214]. Как отмечает автор, «например, при осмотре запущенных в операционной системе процессов или лог-файлов, свидетельствующих о произошедших действиях, описании программного обеспечения, установленного на средства компьютерной техники, достаточно просто перейти к поисковой направленности своих действий, тем самым совершить ошибку, связанную с подменой одного следственного действия другим, а именно — обыском»[215].

Подобная подмена во многом обусловлена тем, что в контексте системы невербальных следственных действий их общей задачей является обнаружение и изъятие криминалистически значимой информации, имеющей доказательственное значение для уголовного дела. Однако смешение их процессуальной формы

---

[213] См.: Пропастин С. В. Осмотр, обыск или судебная экспертиза: проблема выбора при расследовании преступлений, совершаемых с использованием интернет-технологий // Научный вестник Омской академии МВД России. 2015. № 2. С. 20–23.

[214] См.: Поляков В. В., Никитин А. С. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно процессуальными, криминалистическими и оперативно розыскными средствами : сборник научных статей / отв. ред. С. И. Давыдов, В. В. Поляков. Вып. XIV. Барнаул : Изд-во Алт. ун-та, 2017. С. 98.

[215] Поляков В. В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. 2017. № 21. С. 14–17.

недопустимо, поскольку тактические задачи и границы поисковых действий при осмотре и обыске существенно различаются.

Впрочем, как показали результаты обобщения правоприменительной практики, методы, применяемые в ходе данных следственных действий, разнообразны. Порой они предполагают использование специальных знаний. Отчасти это обусловлено природой виртуальных следов, с которыми приходится сталкиваться следователю при реализации поисковых следственных действий.

Отсюда возникает сопутствующая проблема – попытки следователей получить доказательственную информацию в рамках осмотра предметов с использованием специальных знаний. Однако возможности такого предварительного исследования электронных носителей информации существенно ограничены процессуальными рамками осмотра. Если возникающие вопросы выходят за пределы юридических знаний следователя и требуют анализа содержимого электронного носителя информации, единственным возможным решением становится назначение судебной компьютерной экспертизы. Это учитывает и законодатель, регламентируя в ч. 2 ст. 164.1 УПК РФ обязанность привлечения специалиста к производству тех следственных действий, в ходе которых изымаются электронные носители информации, и часть вопросов может быть разрешена уже в процессе осмотра. Однако функции специалиста на данном этапе носят прежде всего обеспечительный характер: они ограничены грамотным изъятием, фиксацией и описанием внешних, «видимых» признаков виртуальных следов. Полноценное же исследование содержимого электронного носителя информации, в том числе скрытого, требует применения специальных экспертных методик, выходящих за рамки компетенции специалиста, и составляет исключительную прерогативу судебного эксперта.

Экспертиза предполагает системный анализ объектов, использование научных методов, фиксацию всех этапов исследования. Это позволяет получить всестороннюю картину и минимизировать риск ошибок. Заключение эксперта, как правило, воспринимается судом как более весомое и объективное доказательство по сравнению с заключением специалиста, который лишь высказал суждение.

Однако ключевая проблема заключается в уголовно-процессуальной форме легализации результатов исследования цифровой информации. В связи с этим именно заключение эксперта выступает наиболее оптимальной процессуальной формой введения полученных сведений в доказательственную базу по уголовному делу.

Специфика виртуальных следов, выходящая за классические представления о механизме следообразования, обусловливает не созерцательно-описательную деятельность субъекта их познания, а поисково-преобразовательную, требующую различных последовательных и параллельных комбинированных шагов по преобразованию информации, опосредованно наблюдаемой при помощи аппаратно-программных средств. В такой ситуации возникает определенный тактический и процессуальный риск: если следователь полностью передает инициативу специалисту, который производит недоступные для понимания следователя манипуляции с программным обеспечением электронного носителя информации, тактическая роль следователя теряется. В результате следователь фактически превращается в стороннего наблюдателя при проведении следственного действия, которое он сам инициировал. Он вынужден фиксировать порой субъективные выводы и умозаключения специалиста, что противоречит принципу объективности фиксации результатов следственного осмотра. Более того, подобное замещение роли следователя на практике нивелирует тактические возможности использования результатов последующей судебной компьютерной экспертизы. Это в дальнейшем порождает конкуренцию выводов, содержащихся в протоколе осмотра и в заключении эксперта, что активно используется стороной защиты.

При этом необходимо учитывать, что участие специалиста не всегда обеспечивает решение всего комплекса задач в процессе конкретного следственного действия. Зачастую для получения криминалистически значимой информации требуются манипуляции, связанные с изменением первоначального состояния объекта, например для получения доступа к заблокированным или

скрытым данным. Решение таких задач относится к компетенции судебного эксперта.

Следственный осмотр ограничивается визуальной фиксацией информации в ее неизменном первоначальном виде, тогда как в рамках судебной компьютерной экспертизы допустимо применение активных методов, связанных с программной или аппаратной модификацией исследуемого объекта.

Таким образом, если при работе с электронными носителями информации следователь приходит к выводу, что получение полного объема сведений невозможно без изменения первоначального состояния объекта или преодоления систем его защиты, объект необходимо направлять для проведения судебной экспертизы. Любые попытки самостоятельного преодоления данных технических барьеров создают неустранимый риск повреждения (уничтожения) виртуальных следов и признания полученных доказательств недопустимыми.

Исключение из этого правила составляет закрепленная в ст. 164.1 УПК РФ процедура копирования информации. В случае ходатайства законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется ее копирование. В протоколе делается запись об этом.

Итогом реализации как следственного осмотра, так и экспертизы является доказательство по уголовному делу. Однако выбор последовательности проведения данных следственных действий в большинстве случаев определяется следователем. И здесь он должен учитывать, что судебная экспертиза является самостоятельным процессуальным следственным действием, однако по отношению к осмотру или обыску она носит производный характер. Экспертное исследование позволяет проверить и объективизировать результаты, полученные следователем в ходе других следственных действий, т.к. выводы эксперта детализируют, подтверждают или опровергают первично зафиксированные сведения. Более того, успешность судебной экспертизы напрямую зависит от того,

насколько качественно и правильно были обнаружены, зафиксированы, изъяты электронные носители информации в ходе невербальных следственных действий.

Таким образом, применительно к работе с электронными носителями информации тактическое решение о выборе между следственным осмотром и судебной экспертизой принимается в зависимости от уровня специальных знаний, необходимого для детального изучения содержания, фиксации виртуальных следов и получения доказательственной информации.

Что касается обыска, то это следственное действие прежде всего предусматривает цель, связанную с отысканием конкретного интересующего объекта в рамках расследуемого преступления, когда предполагается, что он находится в определенном месте, на определенном техническом устройстве и у конкретного человека.

Разделение осмотра и обыска при обнаружении и изъятии электронной информации остается предметом дискуссий в доктрине и судебно-следственной практике. Разграничение между данными следственными действиями проводилось учеными по различным критериям: объектам обнаружения (И. А. Попов, Г. В. Костылева и Н. Е. Муженская)[216], возможности и природе принудительных действий (А. П. Рыжаков)[217], наличию доступа к объектам и защите конституционных прав граждан (А. В. Смирнов и К. Б. Калиновский, Р. И. Оконенко, В. С. Черкасов)[218], комплексному критерию принуждения и доступности (Ю. В. Гаврилин и А. А. Балашова)[219].

В рамках настоящего исследования указанные критерии также применимы, однако требуют адаптации с учетом специфики объекта следственных действий —

---

[216] См.: Руководство для следователя по осмотру места происшествия : учебно-практическое пособие / под ред. И. А. Попова, Г. В. Костылевой, Н. Е. Муженской. М. : Проспект, 2010. С. 7–8.

[217] См.: Рыжаков А. П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации. М. : Гарант-сервис-университет, 2014. С. 635.

[218] См.: Смирнов А. В., Калиновский К. Б. Следственные действия в российском уголовном процессе : учебное пособие. СПб. : СПбГИЭУ, 2004. С. 12 ; Оконенко Р. И. К вопросу о правомерности осмотра компьютера как следственного действия // Адвокат. 2015. № 1. С. 29 ; Черкасов В. С. Проблема разграничения следственных действий: осмотр и обыск при получении компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 99–104.

[219] См.: Гаврилин Ю. В., Балашова А. А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 129–137.

информации, заключенной в ресурсах сети «Интернет». Специфическая природа данных сведений и архитектура информационных систем, в которых они циркулируют, накладывают существенный отпечаток на тактику их обнаружения, обеспечение санкционированного доступа, а также на методы их проверки и сохранения.

По мнению Ю. В. Гаврилина и А. А. Балашовой, различие между осмотром и обыском сто́ит проводить по возможности принудительного обследования информационных систем, доступ к которым ограничен их администраторами или пользователями. Получение общедоступной неограниченному количеству лиц информации, размещенной лицом в открытом доступе без средств парольной и иной защиты, должно осуществляться в рамках процедуры осмотра. Если же доступ ограничен средствами парольной, криптографической и иной защиты, необходимо проводить обыск[220].

Таким образом, вопрос выбора следственного действия большинство авторов связывает с ситуационными особенностями работы с электронными носителями информации. Как показало обобщение следственной практики, такие ситуации можно классифицировать по различным основаниям: по степени угрозы сохранности данных (если есть опасность изменения или уничтожения информации), по техническому состоянию объекта (включен или выключен), по готовности владельца к сотрудничеству (имеется ли добровольное согласие на предоставление доступа к устройству, оказывается ли противодействие расследованию), по правовому статусу объекта (является ли носитель личной собственностью или принадлежит организации) и др.

Наиболее часто на практике складывается ситуация, когда лицо отказывается добровольно предоставить следователю пароли и доступ к устройству. Поскольку принудить к выдаче пароля следователь не может, в подобной ситуации целесообразно ограничиться следственным осмотром устройства с его последующим изъятием и назначением судебной компьютерной экспертизы.

---

[220] См.: Гаврилин Ю. В., Балашова А. А. Указ. соч. С. 134–135.

Ситуация может осложниться тем, что подозреваемый может создать видимость добровольности предоставления доступа к устройству. Следователю необходимо тщательно взвешивать подобные действия, поскольку лицо может таким образом противодействовать получению криминалистически значимой информации и умышленно затягивать процесс расследования. В частности, подозреваемый может добровольно предоставить неверный пароль, введение которого приведет к автоматической блокировке устройства, либо предоставить доступ, а впоследствии заявить ходатайство о нарушении его прав на конфиденциальную информацию. В подобных ситуациях следователю целесообразно подробно зафиксировать в протоколе следственного действия следующие аспекты: факт «добровольного» сообщения пароля подозреваемым и его точное содержание, количество попыток ввода указанного пароля, факт непринятия пароля устройством, факт блокировки устройства.

В этой ситуации мы солидарны с мнением Р. И. Оконенко, который предлагает оценивать свободу доступа с позиции степени вторжения в частную жизнь человека, исходя из его разумного ожидания относительно сохранности тайны его личной жизни[221].

Развивая эту мысль, необходимо разграничить осмотр публичного интернет-пространства и осмотр персональных данных. Для получения и фиксации сведений, находящихся на открытых интернет-ресурсах, доступ к которым не ограничен средствами защиты, осмотр является единственно верной и достаточной формой закрепления доказательств. Напротив, в отношении личных персональных устройств или закрытых аккаунтов даже добровольное согласие лица на передачу паролей не отменяет факта глубокого вторжения в сферу его частной жизни. Даже получив согласие лица на осмотр его телефона или компьютера и необходимые пароли, следователь вторгается в частную жизнь, ограничивая конституционное право на ее неприкосновенность, в связи с чем о свободном доступе не может быть

[221] См.: Оконенко Р. И. К вопросу о правомерности осмотра компьютера как следственного действия. С. 29.

и речи[222]. В этом ключе мы согласны с теми авторами, которые считают, что зачастую целесообразно избирать обыск единственно правильной процессуальной формой для обнаружения информации на персональных программно-аппаратных устройствах или в компьютерных сетях[223].

Более того, инициирование следователем перед судом ходатайства о производстве обыска (в порядке ст. 165 УПК РФ) полностью устраняет риск того, что лицо в дальнейшем оспорит свое «добровольное» согласие. Это гарантирует законность производства данного следственного действия и исключает возможность признания его результатов недопустимым доказательством.

Таким образом, для разрешения проблемы выбора конкретного вида следственного действия и его тактических приемов, применимых в целях получения криминалистически значимой информации в сети «Интернет», необходимо исходить из алгоритма принятия решения, определяющего оптимальную последовательность выбора того или иного следственного действия в зависимости от сложности доступа к сведениям на устройстве, степени их конфиденциальности и характера вторжения в сферу частной жизни граждан.

Переходя к анализу решения обеспечительных задач при работе с ресурсами сети «Интернет», следует отметить, что Сеть позволяет следователю в ходе следственного действия:

— обеспечить удаленный доступ к источнику криминалистически значимой информации (13 %);

— осуществить ориентирование на местности (34 %);

---

[222] Согласно позиции Конституционного Суда РФ получение имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения (определение Конституционного Суда РФ от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации» // СПС «Гарант»).

[223] См.: Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. … канд. юрид. наук. М., 2016 ; Черкасов В. С. Проблема разграничения следственных действий ; Попов А. М., Дубовицкий А. И. Особенности производства осмотра по преступлениям в сфере компьютерной информации как элемент доказывания // Право: история и современность. 2020. № 1 (10). С. 109–115.

— организовать дистанционное производство следственного действия (17 %);

— обеспечить анализ результатов следственного действия (36 %).

При рассмотрении обеспечительных задач использования сети «Интернет» при производстве следственных действий требуется определение дополнительных критериев, т.к. в отличие от поисково-познавательных задач обеспечительные направлены на получение доказательственной информации опосредованно. Здесь сеть «Интернет» выступает преимущественно как средство получения доказательств, которое должно отвечать требованиям, предъявляемым к технико-криминалистическим средствам и технологиям. Из всех выделяемых криминалистами подобных требований[224] для сети «Интернет» наиболее применимы положения научной обоснованности, надежности и квалифицированного применения.

Требование научной обоснованности означает, что любые аппаратно-программные средства, используемые следователем для обеспечения условий производства следственного действия (например, для удаленного подключения к сетевому ресурсу с целью копирования информации и ее последующего осмотра и т.д.), должны быть признаны наукой и апробированы в судебно-следственной практике.

Следует отметить, что требование научной обоснованности вызывает острую дискуссию применительно к аналитическому обеспечению следственных действий, осуществляемому при получении криминалистически значимой информации из ресурсов сети «Интернет» посредством программ на базе искусственного интеллекта. На эту тему имеется достаточно публикаций, в том числе научно-криминалистического характера[225].

---

[224] См.: Вандер М. Б. Применение научно-технических средств при расследовании преступлений : конспект лекций. 2-е изд., перераб. СПб., 2002. С. 8–10 ; Койсин А. А. Правовые основы применения технико-криминалистических средств на предварительном следствии и в суде // Сибирский юридический вестник. 2007. № 4 ; Скворцов Р. И. Уголовно-процессуальные и тактические основы применения технических средств при производстве следственных действий // Общество и право. 2013. № 4 (46) 2013. С. 188–191 и др.

[225] См.: Меретуков Г. М., Усенко А. С. Особенности использования искусственного интеллекта в криминалистической деятельности: некоторые актуальные вопросы // Вестник Томского государственного университета. Право. 2025. № 57. С. 44–58 ; Фомина И. А. Использование искусственного интеллекта в

В современном уголовном судопроизводстве технологии искусственного интеллекта находят применение по следующим направлениям: поисково-аналитическое (мониторинг ресурсов сети «Интернет», анализ больших данных, распознавание объектов по биометрическим данным), технико-обеспечительное (3D-моделирование места происшествия), прогностическое (выдвижение следственных версий, оценка тактического риска). Внедрение указанных инструментов существенно оптимизирует процесс расследования преступлений, однако требует точной правовой регламентации производимых действий.

Необходимость и неизбежность повышения технологичности деятельности правоохранительных органов вытекают из задач Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10.10.2019 № 490[226].

В рамках экспериментальной части нашего исследования было проведено комплексное изучение отдельных нейросетевых технологий, доступных в сети «Интернет». Целью данного эксперимента выступала проверка надежности и научной обоснованности применения искусственного интеллекта в качестве аналитического ассистента следователя. Для оценки способности искусственного интеллекта систематизировать материалы уголовных дел перед нейросетями был поставлен ряд задач по анализу:

— заключений экспертов по архивным уголовным делам на предмет наличия нарушений и ошибок;

— показаний подозреваемых (обвиняемых), потерпевших и свидетелей с целью выявления совпадений и противоречий;

— заключений экспертиз, показаний и обвинительных заключений на предмет установления полноты расследования;

криминалистическом анализе: отдельные проблемы теории и практики // Сибирский юридический вестник. 2026. № 1 (112). С. 103–109 и др.

[226] СЗ РФ. 2019. № 41. Ст. 5700.

— обвинительных заключений и приговоров в целях выявления обстоятельств предмета доказывания, недостаточно обеспеченных доказательствами.

По итогам проведенного исследования был выявлен факт допущения ошибок нейросетями. К таковым относятся следующие:

1. По характеру:

— терминологические (неверный или неточный выбор юридической и специальной терминологии);

— методологические (ссылки на несуществующие экспертные методики);

— хронологические (ссылки на устаревшие методики экспертного исследования).

2. По объекту анализа:

— ошибки в процессуальных документах (искажение терминологии при анализе показаний, обвинительных заключений);

— в материалах судебных экспертиз (неверные выводы, методологические искажения при анализе заключений экспертов).

3. По степени сложности выявления:

— очевидные (выявляются квалифицированным юристом самостоятельно);

— сложноверифицируемые (требуют привлечения ученых и специалистов в узких областях знаний для оценки корректности выводов нейросети).

В то же время полученные данные исследования возможностей нейросетей при анализе результатов отдельных следственных действий и их совокупности демонстрируют, что аналитическое направление в обеспечительной функции использования сети «Интернет» в тактике следственных действий позволяет правоприменителю оценить степень достижения целей как отдельных тактических задач, так и всего расследования. Примечательно, что адвокатский корпус уже относительно давно использует нейросети для выявления ошибок в действиях следователей. На специальной конференции, посвященной правовым аспектам

искусственного интеллекта[227], вопросам использования нейросетей в деятельности адвокатов по уголовным делам была посвящена отдельная секция, где практикующие юристы активно обсуждали успешный опыт машинного определения различных недочетов предварительного расследования и судебного разбирательства. Целесообразно рекомендовать следователям активно внедрять в практику расследования преступлений аналитические возможности нейросетевых технологий. Это позволит самостоятельно выявлять допущенные ошибки или неполноту сведений, своевременно устранять их, а также действовать на упреждение со стороны лиц, оказывающих противодействие расследованию.

Следует отметить, что требование научной обоснованности неразрывно связано с требованием надежности. При этом надежность в сети «Интернет» не всегда зависит от выбранных научных подходов и инструментов: зачастую она обусловлена прохождением и устойчивостью электронного сигнала, а также способностью субъекта расследования технически обеспечить эту стабильность, что напрямую актуализирует и критерий квалифицированного применения интернет-технологий. Данная взаимосвязь приобретает особую значимость при реализации таких обеспечительных задач, как удаленный доступ к источникам криминалистически значимой информации, ориентирование на местности и дистанционное производство следственных действий.

На практике перед следователем зачастую возникает вопрос, связанный с тем, что необходимая для расследования преступления информация труднодоступна для осмотра или обыска, т.к. может находиться на удаленном сервере в сети «Интернет» или в облачном хранилище[228]. Обнаружение и осмотр такой компьютерной информации иногда оформляются как осмотр места происшествия, несмотря на то, что происходят в служебном кабинете следователя с использованием служебной компьютерной техники[229]. В этом аспекте актуальны

---

[227] Форум «ПравоТех» (25 сентября 2025 г.) [Электронный ресурс] // URL: pravo.tech (дата обращения: 11.04.2026).

[228] См.: Попов А. М., Дубовицкий А. И. Указ. соч. С. 109–115.

[229] См.: Стельмах В. Ю. Современные проблемы фиксации хода и результатов производства следственных действий и возможные пути их решения // Актуальные проблемы российского права. 2016. № 7. С. 152–159.

современные научные дискуссии об осуществлении изъятия электронной информации в рамках обыска в дистанционном режиме, т.е. удаленно.

Суть данной технологии заключается в том, что, располагая специальным программным обеспечением, следователь с помощью специалиста может «проникнуть» в любой компьютер, ознакомиться с имеющимися в нем файлами, а также отыскать необходимую для следствия информацию. Следует отметить, что такой способ получения доказательственной информации используется правоохранительными органами многих стран (например, в Германии — для раскрытия и расследования наиболее опасных преступлений). Будучи аналогичной по своей природе вирусу «троянский конь», программа распространяется через сеть «Интернет» и, поразив нужный компьютер, позволяет следить за активностью его пользователя в интернет-браузерах, программах связи типа Skype, электронной почте и чатах, другими словами, обеспечивает производство «электронного обыска»[230].

Действующим российским уголовно-процессуальным законодательством проведение подобных дистанционных следственных действий не предусмотрено, а схожие мероприятия регламентированы Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности». В свою очередь, отечественный уголовный процесс имеет опыт внедрения дистанционных технологий в производство следственных действий (например, допрос с использованием видео-конференц-связи (ВКС)).

Впрочем, мы полагаем, что использование технологий удаленного доступа к компьютерной информации, в частности дистанционный обыск, может быть эффективным и обладает следующими преимуществами:

— возможность получения доказательственной информации по уголовному делу непосредственно на своем рабочем месте, что экономит ресурсы сотрудников правоохранительных органов и оптимизирует ход расследования;

---

[230] См.: Ищенко Е. П. О насущных проблемах раскрытия и расследования преступлений // Вестник Восточно-Сибирского института МВД России. 2017. № 3. С. 134.

— возможность проведения дистанционного обыска устройства, находящегося в ином регионе или даже за пределами России;

— обеспечение фактора внезапности при производстве «дистанционного» обыска, что позволяет максимально исключить проблему, связанную с безвозвратным удалением интересующих сведений с электронных носителей информации. Как показывает практика, лица, причастные к преступлению и хранящие у себя электронные носители информации, обычно тщательно проинструктированы о порядке действий по уничтожению данных на случай визита к ним сотрудников правоохранительных органов.

Обозначая эффективность и практическую значимость данного следственного действия, следует отметить, что возникает вопрос о правомерности получения в его рамках интересующей информации. Ведь в процессе дистанционного обыска происходит проникновение в другой компьютер, в ходе которого подбираются пароли и используется специальное программное обеспечение. Тем самым осуществляется так называемый взлом при помощи программно-аппаратных комплексов, к числу которых С. Ю. Скобелин относит «универсальное устройство извлечения судебной информации (UFED — Universal Forensic Extraction Device), мобильный криминалист, XRY, MOBILedit», «Тарантул» и др.[231], что может быть аналогично вскрытию помещений. В данном случае опять возникает вопрос о том, имеется ли необходимость получать судебное решение на производство такого действия в целях недопущения нарушения конституционных прав граждан. Другая же проблема — отсутствие нормативной процедуры дистанционного обыска, что также может привести к признанию полученного таким способом доказательства недопустимым.

Достаточно подробно проблему дистанционного обыска исследовала А. А. Балашова, которая под ним понимает «следственное действие, состоящее в принудительном обследовании информационной системы, находящейся на электронных носителях за пределами места производства следственного действия,

[231] Скобелин С. Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 32.

доступ к которым ограничен ее обладателем и осуществляется посредством компьютерных сетей»[232]. Ученый предлагает дополнить гл. 25 УПК РФ статьей 182.1 «Дистанционный обыск» и приводит редакцию соответствующей нормы. Примечательно, что А. А. Балашова выделяет объект процессуальных поисковых действий — информационные ресурсы, поскольку его отсутствие в настоящее время в уголовно-процессуальном законе (ограниченном перечнем только из двух объектов: какое-либо место или лицо, где могут находиться имеющие значение для дела орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, разыскиваемые лица, трупы или информация о них) создает правовое препятствие в процедуре такого рода.

Сомнение вызывает необходимость внесения целой статьи, основными положениями дублирующей порядок производства обычного обыска. На наш взгляд, с точки зрения законодательной техники правильнее было бы предложить дополнения к ст. 182 УПК РФ, в которых закрепить особенности обыска удаленных информационных ресурсов, а также порядок предъявления постановления (если физический контакт с обладателем информации/устройства невозможен или существует риск удаленного уничтожения данных соучастниками, постановление предъявляется лицу сразу после фактического получения доступа к информационному ресурсу и фиксации виртуальных следов). Такой подход позволит адаптировать право к цифровым реалиям, избежав дублирования норм и излишней перегрузки уголовно-процессуального закона.

Полагаем, в данном случае участие специалиста является обязательным, и предлагаем следующий порядок действий при дистанционном обыске:

1) установить IP-адрес соединения между устройством и сетью «Интернет» и физический адрес (MAC-адрес). Необходимо обратить внимание, что физический адрес может быть «подменен» средствами операционной системы, и об этом не следует забывать;

---

[232] Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : автореф. дис. … канд. юрид. наук. М., 2020. С. 24–25.

2) изучить данные браузера, который использовался интересующим следствие лицом для доступа к ресурсам (запросы, обработка, отображение содержания и просмотр сайтов, обмен файлами с серверами и т.п.). Изучение браузера следует проводить с осторожностью и не закрывать открытые вкладки, т.к. это может привести к прекращению сеанса работы с сервисом, требующим ввода пароля;

3) преодолеть, при наличии, технические и программные средства ограничения доступа к компьютерной информации;

4) изучить информацию об истории просмотра веб-страниц и закладок в браузере (особо обратить внимание на социальные сети, посещавшиеся пользователем сайты и информацию на них, а также на электронные платежные системы, которыми пользовалось интересующее следствие лицо (WebMoney, Bitcoin и др.));

5) изучить электронную почту, в ходе чего следует установить историю переписки (особенно в части преступной деятельности и соответствующих связей), контакты других лиц, доступ к иным сетевым службам, а также обратить внимание на содержимое папок «Спам», «Черновики», «Удаленные». В ходе исследования почты возможно восстановить пароли доступа к форумам, электронным платежным системам и пр.;

6) исследовать средства синхронизации данных (например, «Яндекс.Диск», «VK Cloud» и др.), которые позволяют помимо локального хранения файлов пользователя размещать информацию на нескольких компьютерах и в сети, где могут быть сохранены удаленные из памяти компьютера файлы, контакты и др. Поскольку синхронизация может производиться без команды пользователя (например, при подключении телефона к компьютеру), это обстоятельство имеет существенное криминалистическое значение, т.к. удаленные с персонального устройства файлы пользователя могут без его ведома остаться в синхронизированном «облаке»;

7) выявить средства анонимизации. К ним относится программное обеспечение для сокрытия личных данных и следов пребывания пользователя в сети «Интернет», о котором мы писали ранее;

8) применить средства поиска файлов, что можно сделать с помощью встроенных возможностей операционных систем по имени файла, дате последнего изменения, его типу, а также по содержимому файлов;

9) восстановить недавно удаленную информацию, если это не требует использования специального программного обеспечения (которое необходимо применять уже при производстве судебной экспертизы). В используемых операционных системах при удалении файлы попадают в «корзину», из которой они могут быть извлечены обратно и восстановлены без каких-либо специальных средств. При очистке «корзины» информация все еще будет храниться в системе, пока на освобожденный участок носителя не будет записана новая информация. В этом случае следует применить специальное программное обеспечение, позволяющее восстановить удаленную, но не перезаписанную информацию (R.saver, Recuva, RecoverMyFiles и др.). В связи с этим рекомендуется до восстановления недавно удаленных файлов не производить копирование новых данных и не запускать программы, занимающие большой объем памяти, чтобы исключить утрату возможности восстановления информации;

10) обнаруженную и подлежащую изъятию в ходе обыска информацию следует скопировать на электронный носитель, который необходимо упаковать и оформить по правилам уголовного судопроизводства, исключающим его повреждение или подмену. Здесь мы полностью согласны с Ю. В. Гаврилиным и А. А. Балашовой в том, что изъятие выявленной в ходе дистанционного обыска доказательственной информации, находящейся в компьютерных сетях, возможно только путем ее копирования, поскольку отсутствует непосредственный физический доступ к носителям, на которых находятся имеющие значение для уголовного дела сведения. Исходная же информация остается в неизменном состоянии, а скопированная информация тождественна оригиналу и является

источником доказательств[233]. Возможные сомнения стороны защиты в тождественности скопированной информации могут быть устранены за счет обращения к специальным знаниям. Специалист при копировании данных сразу может принимать меры, которые делают сомнения в подлинности необоснованными: использовать носители информации, на которые невозможно вносить изменения после записи, фиксировать хеш-суммы и др. Здесь следует отметить, что программное обеспечение должно быть лицензированным, а средства измерений, применяемые при осуществлении судебно-экспертной деятельности, должны поверяться только аккредитованными в установленном порядке в области обеспечения единства измерений государственными региональными центрами метрологии в соответствии с постановлением Правительства РФ от 20.04.2010 № 250 «О перечне средств измерений, поверка которых осуществляется только аккредитованными в установленном порядке в области обеспечения единства измерений государственными региональными центрами метрологии»;

11) если в ходе обыска были предприняты попытки уничтожить исследуемую информацию, необходимо описать соответствующие действия и принятые меры.

Следует отметить, что большинство из описанных действий зачастую требует специальных знаний и возможностей оперативно-разыскной деятельности. Поэтому взаимодействие со специалистами и с органами, осуществляющими оперативно-разыскную деятельность, имеет ключевое значение для достижения целей дистанционного обыска.

В зависимости от вида расследуемой преступной деятельности и отражающей ее в компьютерных сетях криминалистически значимой информации предложенный алгоритм должен быть конкретизирован с указанием содержания искомых сведений.

В развитие изложенного отметим, что при выполнении ранее выделенной обеспечительной задачи при реализации невербальных следственных действий,

[233] См.: Гаврилин Ю. В., Балашова А. А. Указ. соч. С. 136.

проводимых с использованием сети «Интернет», также имеет значение такое техническое требование, как надежность интернет-сигнала. Данное условие напрямую влияет на возможности проведения ряда дистанционных следственных действий.

Необходимо также учитывать, что интернет-сигнал напрямую связан с технологией навигации. Последняя позволяет точно определить, где именно находится устройство во время следственных действий.

Согласно Федеральному закону от 14.02.2009 № 22-ФЗ «О навигационной деятельности»[234] под средствами навигации понимаются технические средства, устройства и системы, предназначенные для формирования навигационных сигналов, передачи, приема, обработки, хранения и визуализации навигационной информации. В практике расследования встречаются ситуации, когда, например, осмотр или проверка показаний на месте проводятся в местах, отдаленных от каких-либо ориентиров, привязанных к местности. Соответственно, первоначально сложно определить точные данные местоположения участников следственного действия на территории. Такие сведения необходимо устанавливать, поскольку определение места совершения преступления входит в объем обстоятельств, подлежащих доказыванию. Как правило, для решения задачи, связанной с точным определением адресных координат осматриваемой территории, используется мобильный телефон (смартфон) с доступом в сеть «Интернет»: 1) посредством использования функции GPS, позволяющей определять местоположение по координатам сети либо по спутникам GPS. Сто́ит отметить, что в случае неполадок с сетью определить координаты при отсутствии сигналов от спутников GPS не представляется возможным. Альтернативным, по нашему мнению, будет предложение А. В. Рудневского по определению местоположения по базовым станциям GSM-сети[235]; 2) посредством использования специального программного обеспечения / интернет-приложений по определению местоположения устройства

[234] СЗ РФ. 2009. № 7. Ст. 790.

[235] См.: Рудневский А. В. Определение местоположения по базовым станциям в сетях GSM // Беспроводные технологии. 2010. № 20. Т. 3. С. 16–18.

(«Моя GPS позиция», «Яндекс Карты» и др.). Примечательно, что данные о местоположении мобильного телефона и его перемещении автоматически передаются на серверы компании, которая предоставляет услуги геолокации, или сохраняются в памяти телефона. Соответственно, возможности получения сведений о местоположении не только помогают следователю установить точные координаты места, на котором производится следственное действие, но и являются поводом для проведения осмотра мобильного телефона предполагаемого подозреваемого (обвиняемого) и направления его на судебную компьютерную экспертизу с целью обнаружения сведений о местоположении телефона лица в интересующий момент времени и сопоставления их с данными, указанными следователем в протоколе осмотра, для установления причастности лица к совершенному преступлению и получения иных доказательств.

Кроме этого, интернет-приложения по определению местоположения устройства позволяют решать дополнительную задачу по установлению криминалистически значимой информации, когда в рамках подготовки и проведения следственного действия следователь по цифровой карте может выявить камеры видеорегистрации, находящиеся вблизи интересующего следствие места, и в последующем получить с них запись того дня, когда происходило расследуемое событие. Например, гр-н А., подозреваемый в убийстве и отрицавший свою причастность, в ходе проверки показаний на месте рассказал о маршруте их движения с жертвой. Полученные в ходе проверки GPS-координаты не вполне совпадали с координатами точек геолокации телефона жертвы в день исчезновения. В последующем обвиняемый А. пояснил, что до момента задержания он проехал по маршруту дня убийства и специально фиксировал, где находятся камеры уличного наблюдения, в обзор которых он попадал вместе с жертвой, чтобы для возможной проверки показаний выстроить параллельный, не отслеживаемый камерами маршрут. Если бы органы следствия воспользовались приложением «Яндекс Карты», то они обязательно обратили бы внимание на то,

что маршрут проверки его показаний был построен так, чтобы объезжать камеры дорожной фиксации, АЗС, торговые комплексы и учреждения[236].

Вместе с тем в развитие требования надежности следует также указать на важность требования квалифицированного применения интернет-технологий, которое носит междисциплинарный характер. Согласно ему субъект расследования должен обладать не только базовой компьютерной грамотностью, но и специальными знаниями и навыками в сфере информационных технологий. Следователь должен понимать архитектуру сети «Интернет», принципы маршрутизации и механизмы работы сетевых протоколов. Это необходимо для объективной оценки состояния Сети, своевременного выявления сбоев или подмены электронных данных, а также для корректировки порядка действий при работе с ними.

Практически в каждом тезисе настоящего параграфа затрагиваются аспекты, связанные с необходимостью использования специальных компьютерно-технических знаний, без которых производство следственных действий с использованием сети «Интернет» невозможно. Безусловно, это должно осуществляться за счет обращения к сведущим лицам, чья помощь облекается в процессуальные рамки привлечения специалиста и назначения экспертизы. Однако очевидно, что помощь этих лиц по тем категориям следственных действий, в рамках которых используется сеть «Интернет», перманентна. Данный фактор обусловливает потребность в значительном штате профильных специалистов, сопоставимом по численности со следователями, расследующими преступления, в которых фигурирует сеть «Интернет». Как следствие, на первый план выходит вопрос не только количественного кадрового обеспечения, но и формирования у самих субъектов расследования надлежащих компетенций в области квалифицированного использования сети «Интернет».

В современных условиях лицу, производящему расследование, недостаточно обладать исключительно базовыми юридическими знаниями. Следователь должен

[236] Материалы уголовного дела № 1-22/2013 // Архив Тюменского районного суда Тюменской области за 2013 г.

иметь уровень подготовки, позволяющий объективно оценить квалификацию специалиста, привлекаемого для обнаружения и фиксации электронных криминалистически значимых сведений либо оказывающего техническое содействие при производстве соответствующих следственных действий.

Это обусловливает потребность в повышении квалификации следователей в направлении работы с электронной информацией и сетью «Интернет». На наш взгляд, нецелесообразно создавать или расширять соответствующие подразделения в структуре следственных органов, которые занимались бы только расследованием так называемых киберпреступлений, поскольку существование электронной криминалистически значимой информации стало нормой практически по каждому преступлению. Конечно, для расследования особо сложных киберпреступлений такие подразделения должны быть, но современное развитие технологий диктует необходимость их углубленного изучения всеми юристами. Соответственно, целесообразнее организовать дополнительное обучение в рамках специальных курсов по технологиям получения и использования в расследовании электронной информации.

В данном плане мы поддерживаем предложение Л. В. Бертовского о необходимости введения в образовательные программы дисциплин уголовно-правового профиля специализации, отражающей технический аспект данной проблематики (использование больших данных в энергетических секторах, нейротехнологий и искусственного интеллекта, возможностей робототехники и сенсорики, применяемых в сфере энергетики; технологий беспроводной связи, виртуальной и дополненной реальностей и др.)[237].

Подводя промежуточный итог анализу поисково-познавательных и обеспечительных задач тактики реализации невербальных следственных действий, проводимых с использованием сети «Интернет», полагаем необходимым сформулировать систему их специальных принципов. Принципы являются

[237] Бертовский Л. В. О некоторых проблемах расследования преступлений, совершаемых в сфере энергетики // Криминалистические чтения на Слобожанщине : сборник материалов Международной научно-практической конференции, Белгород, 8 октября 2021 г. / под ред. Н. А. Жуковой. Белгород : ИД «БелГУ» НИУ «БелГУ», 2021. С. 3–7.

основополагающим компонентом любой теоретической системы наряду с ее законами и категориями. С практической точки зрения именно принципы формируют содержание конкретной деятельности и носят конструктивный характер, т.к. из них конструируется модель определенного поведения.

Данные положения отсылают нас к высказыванию Р. С. Белкина о том, что при построении любой классификации принципов необходимо четко и однозначно понимать, в каком смысле о них будет идти речь, не пытаясь втиснуть в рамки этого определения иные значения данного понятия[238]. Иными словами, в основе подразделения принципов проведения следственных действий должны лежать единые критерии, исходя из которых будут определяться их отличительные признаки и осуществляться классификация.

Начнем с принципа юридической адресности. Данный принцип означает, что выбор конкретного следственного действия и тактики его проведения должен быть обусловлен закономерной связью правового статуса виртуального пространства и технического режима доступа к интересующим сведениям. Следователю необходимо предварительно оценить категорию ресурса сети «Интернет» для исключения ситуации подмены одного следственного действия другим, что может привести к признанию полученного доказательства недопустимым.

Интернет-ресурсы классифицируются по различным основаниям, в том числе по характеру данных (контент, метаданные, инфраструктурные данные) и правовому режиму доступа (открытые, условно-открытые, закрытые, анонимизированные). Соответственно, когда ресурс находится в открытом доступе (например, контент конкретной страницы сайта), безусловно необходимо провести осмотр интернет-страницы с целью фиксации имеющихся сведений. Вместе с тем в следственной практике нередко возникают ситуации, когда искомая информация находится в анонимизированном сегменте сети «Интернет». Проникновение в такой ресурс в рамках процессуальной формы требует специальных знаний и

[238] Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М. : Юрид. лит., 1987. С. 27.

аппаратно-программных средств, что предполагает назначение и производство экспертизы.

В свою очередь, метаданные, сетевые и операторские сведения относятся к условно-открытым и преимущественно к закрытым типам доступа, что предполагает реализацию механизма процессуального принуждения при их получении и, соответственно, вызывает необходимость производства выемки и обыска.

Принцип юридической адресности тесно переплетается и взаимосвязан с другими принципами следственных действий. В частности, очевидна тесная связь с принципом законности, поскольку направление запроса организатору распространения информации в сети «Интернет» (с целью получения переписки пользователей и иной криминалистически значимой информации) зачастую сопряжено с ограничением конституционных прав граждан на тайну переписки и неприкосновенность частной жизни. Это, в свою очередь, предопределяет необходимость обращения за дополнительной гарантией соблюдения законности в виде судебного решения на производство следственных действий.

В развитие изложенной позиции В. С. Черкасовым выдвинуты достаточно убедительные предложения и обоснованные изменения и дополнения к уголовно-процессуальному закону, касающиеся порядка действий органов расследования при получении электронной информации[239]. В частности, ученым аргументирована необходимость совершенствования следственных действий, ограничивающих конституционные права граждан на тайну переписки и телефонных переговоров. Им также предложен новый механизм изъятия цифровой информации, адаптированный к условиям трансграничности сетевой инфраструктуры, позволяющий получать необходимые сведения в кратчайшие сроки, т.е. путем удаленного копирования, независимо от физического местонахождения сервера.

Вопрос выбора процессуального способа получения электронной информации из сети «Интернет» обусловлен также и особенностями самой

[239] См.: Черкасов В. С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса : дис. … канд. юрид. наук. Хабаровск, 2022.

информации. Быстрая изменяемость интернет-сведений приводит к тому, что публикации удаляются, объявления и ссылки исчезают, контент персонализируется и деперсонализируется. Данные обстоятельства детерминированы принципом ситуативности проведения следственного действия. Симбиоз этого «классического» принципа с закономерностями функционирования информации в сети «Интернет» позволяет комплексно воздействовать на следственную ситуацию. В частности, это достигается посредством параллельного решения двух задач. Первая — безотлагательное обнаружение и фиксация открытого и быстроизменяемого контента путем проведения следственного осмотра. Вторая — получение сведений от операторов связи и организаторов распространения информации в сети «Интернет» посредством обыска или выемки.

Таким образом, ключевым тактическим принципом здесь выступает двухпоточность действий, под которой понимается параллельное проведение разных следственных действий исходя из природы информации, заключенной в сети «Интернет». Первый поток направлен на фиксацию открытых, динамично изменяющихся электронных данных в режиме реального времени на сайте или ином интернет-ресурсе, тогда как второй — на получение сведений, хранящихся на серверах организаторов распространения информации в сети «Интернет» (ч. 7 ст. 185, ст. 186.1 УПК РФ). Синхронизация данных потоков позволяет следователю нивелировать риск утраты криминалистически значимой информации и своевременно фиксировать необходимые сведения. Этот принцип логично вытекает из системности следственных действий, суть которой заключается в синергетическом векторе воздействия на определенные ситуации посредством комплексной методологии разных следственных действий в целях решения конкретных задач расследования.

Полученная при реализации принципа двухпоточности информация из сети «Интернет» должна быть незамедлительно подвергнута осмотру и исследованию, в том числе с участием специалиста. Это позволяет не только установить фактические обстоятельства расследуемого преступления, но и определить источники, а также направления поиска иной криминалистически значимой

информации, содержащейся в сети «Интернет» и на персональных устройствах лиц, имеющих отношение к преступному событию. Исходя из этого возникает необходимость выделения еще одного принципа интеграции сети «Интернет» в тактику следственных действий — тактической оперативности использования информации, полученной посредством сети «Интернет».

Как показали результаты исследования, на практике именно оперативность использования данных из сети «Интернет» при производстве отдельного следственного действия для обоснования и проведения последующих следственных действий выступает ключевой проблемой расследования. Это объясняется тем, что, во-первых, интерпретация таких данных требует специальных познаний и, соответственно, временны́х ресурсов для проведения соответствующих исследований, а во-вторых, сами правоприменители испытывают затруднения в выборе соответствующего специалиста и определении круга его компетенций для решения конкретных тактических задач расследования. Зачастую следователю сложно сразу определить, требуется ли ему специалист в области сетевых технологий, информационной аналитики либо аппаратно-программного исследования устройства.

Реализуя ситуационный подход к интерпретации и применению специальных знаний при проведении следственных действий с использованием ресурсов сети «Интернет», следователь должен объективно оценивать текущую следственную ситуацию и самостоятельно определять необходимость привлечения специалиста. Это обусловлено тем, что информация на электронных носителях может зачастую находиться в форме, недоступной для восприятия и понимания лицом, не обладающим специальными знаниями в области информационных технологий.

Таким образом, участие специалиста становится обязательным условием для корректной интерпретации цифровой информации и ее использования в расследовании преступления.

Сеть «Интернет» как объект познания криминалистической науки сегодня невозможно анализировать без оценки достоверности содержащейся в ее ресурсах электронной информации. Виртуальная среда облегчает получение и

использование поддельных электронных документов и файлов, позволяет манипулировать цифровыми объектами и скрывать внесенные изменения. Специальные исследования последних лет описывают эти способы и подчеркивают необходимость разработки методик выявления фальсификации[240]. В связи с этим к полученным в сети «Интернет» сведениям должны применяться стандарты контрпроверки, предполагающие их независимое подтверждение из нескольких источников, анализ метаданных, сопоставление с инфраструктурными событиями и назначение экспертиз при сомнении в подлинности. Данный комплекс действий представляет собой верификационную процедуру, направленную на установление истинности полученной в Сети криминалистически значимой информации. Тем самым принцип технологической верифицируемости предопределяет выбор и тактику следственных действий, производимых с использованием ресурсов сети «Интернет». Данный принцип тесно переплетен с нормативным требованием достоверности доказательств, согласно которому вовлекаемые в процесс расследования электронные сведения должны соответствовать объективной действительности, быть правдивыми и правильно отражать обстоятельства, подлежащие доказыванию.

В целях предотвращения (либо минимизации рисков) удаления и подмены сведений на устройстве, а равно для успешного решения задач по сохранению криминалистически значимой информации правоохранительным органам необходимо расширять практику применения современных технико-криминалистических средств и методов. В данном контексте логично выделить принцип технического обеспечения минимизации потери информации. В частности, речь идет о снабжении правоприменителей, работающих с электронными носителями информации, экранирующими средствами защиты,

---

[240] См., например: Ефремова М. А., Русскевич Е. А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 97–105 ; Исаева К. А., Калиев Т. Т. Фальсификация доказательств с использованием дипфейк технологий // Аграрное и земельное право. 2024. № 12 (240). С. 460–462 ; Климова Я. А. Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия // Актуальные проблемы российского права. 2025. Т. 20. № 10 (179). С. 133–143 ; Нестеров В. С. Использование цифровых технологий при фальсификации доказательств в досудебном производстве по уголовным делам // Гуманитарные, социально-экономические и общественные науки. 2025. № 8. С. 132–136, и др.

функционирующими по принципу «клетки Фарадея» (чехлы, боксы, палатки и пр.)[241]. Изоляция изъятого устройства в экранирующем чехле непосредственно на месте проведения следственного действия должна стать обязательным элементом алгоритма действий следователя. Это позволяет зафиксировать и сохранить текущее состояние внешней и внутренней стороны устройства. В противном случае, используя функции удаленного доступа, можно инициировать сброс настроек на телефоне до заводских, что повлечет за собой безвозвратную потерю криминалистически значимых сведений.

Вместе с тем обозначенный принцип не должен ограничиваться исключительно пассивным экранированием сигналов. Правоохранительным органам необходимо внедрять специализированные мобильные комплексы для оперативного извлечения данных с устройства, например программное обеспечение «Мобильный Криминалист».

Принцип обеспечения допустимости полученных доказательств. Еще один немаловажный аспект, связанный с сохранением цифровой информации путем ее копирования, — обеспечение ее допустимости. Отсутствие в ч. 3 ст. 164.1 УПК РФ конкретного перечня применимых для этого технических средств закономерно и обусловлено стремительным развитием информационно-телекоммуникационных технологий. Однако базовые требования к техническому инструментарию фиксации цифровой информации нуждаются в законодательном закреплении. В этой связи использование сертифицированного программного обеспечения для копирования информации позволяет зафиксировать данные из устройства до того, как оно разрядится, заблокируется или отключится, что существенно снижает риски последующей невозможности обхода криптографической защиты. Это позволит избежать проблем, связанных с признанием недопустимой для

[241] URL: https://velter.tech/blog/tpost/in1chgep81-kak-produkti-velter-pomogayut-raskrivat (дата обращения: 01.06.2026).

использования в качестве доказательственной полученной с их помощью цифровой криминалистически значимой информации[242].

Руководствуясь выделенными принципами, учитывая специфику и задачи указанных следственных действий, а также в целях формирования доказательственной базы, предлагаем следующее:

1) первоначально осуществлять с участием специалиста осмотр электронных носителей информации, содержащих следы использования сети «Интернет» и контентных интернет-ресурсов (электронная почта, интернет-страницы, мессенджеры), с целью скорейшего закрепления и получения максимального объема доказательственной и ориентирующей информации, а также недопущения потери информации, зафиксированной на этих носителях. Специалисту же, в свою очередь, необходимо в рамках осмотра исследовать информацию, имеющуюся на электронном носителе, чтобы оценить возможность копирования сведений с него без изъятия устройства. Кроме того, объем специальных знаний в области информационных технологий у следователей не всегда позволяет принять верное решение в ситуации, связанной с высоким риском утраты интересующей информации. Такие, как указывает Н. П. Яблоков, «нештатные» ситуации[243] имеют распространенный характер в повседневных реалиях. Поэтому мы полагаем необходимым обязательное привлечение специалиста к проведению данного следственного действия;

2) если доступ к электронному устройству или конкретному интернет-ресурсу ограничен средствами парольной, криптографической и иной защиты, даже при условии их добровольного указания заинтересованным лицом, должен проводиться обыск. В случаях, не терпящих отлагательства, это решение должно быть принято на месте, возможно, в процессе осмотра. По завершении осмотра необходимо незамедлительно вынести постановление о безотлагательном обыске и провести его;

---

[242] Черданцев А. Ю. Практические проблемы получения, анализа и последующей правильной интерпретации полученной цифровой криминалистически значимой информации // Эксперт-криминалист. 2022. № 4. С. 26–29.

[243] См.: Яблоков Н. П. Криминалистика : практикум. М. : Юристъ, 2004. С. 518.

3) при наличии вопросов, которые не могут быть разрешены путем следственного осмотра и обыска, возникает необходимость назначения судебной компьютерной экспертизы для решения отдельных задач расследования. Проблемы, связанные с выявлением следов взаимодействия пользователя с сетью «Интернет» посредством аппаратно-программных устройств, могут изучаться дифференцированно, в зависимости от конкретного объекта анализа: программного обеспечения, электронных данных, компьютерных систем и т.п.

При этом указанные сведения необходимо анализировать так, чтобы исключить их модификацию, т.е. с целью сохранения в первоначальном состоянии. Существуют различные методики, позволяющие исследовать и фиксировать данные в аутентичном виде. В связи с этим целесообразно согласиться с подходом С. И. Кувычкова, предлагающего технологию поиска электронной информации на подключенном к стендовому компьютеру клонированном диске специалиста (эксперта)[244].

Впрочем, практическая реализация данной методики неизбежно ставит перед правоприменителем вопрос о разграничении процедур копирования и клонирования электронных носителей. Несмотря на схожесть в проведении этих процедур, они имеют технические и процессуальные различия, влияющие на полноту получаемых данных и их дальнейшую проверку.

Следует отметить, что в информатике выделяют различные подходы к переносу цифровой информации. Так, копирование рассматривается как базовая операция по созданию дубликата объекта путем побитового переноса его содержимого. В свою очередь, клонирование представляет собой более сложный процесс, который помимо создания копии может включать в себя глубокое копирование вложенных объектов и структур данных. Клонирование позволяет создать точную копию текущего устройства, включая все приложения, настройки и файлы. Это полезно, если есть опасения утраты криминалистически значимой информации из-за случайного удаления, неисправности устройства или сбоя

[244] См.: Кувычков С. И. Указ. соч. С. 76–81.

системы. Например, при клонировании USB-накопителя помимо данных переносятся главная загрузочная запись диска и таблицы разделов. В результате этой процедуры формируется готовый образ, который состоит из всех видимых и скрытых файлов и неиспользуемого пространства диска.

Исходя из этого можно сказать, что выбор между копированием и клонированием информации в ходе следственных действий не является исключительно техническим вопросом, а напрямую определяет полноту и допустимость доказательств и будет обусловлен конкретной следственной ситуацией.

Данный принцип находится в логической связи с принципом воспроизводимости и проверяемости электронной информации. Специфика виртуального пространства заключается в том, что материальный носитель отделен от своего логического содержания. Изъятая информация становится пригодной для доказывания только тогда, когда алгоритм ее фиксации позволяет гарантировать неизменность первоначального состояния данных и обеспечивает техническую возможность их повторного бесконечного отображения без потери качественных характеристик. Фиксация должна позволять «воспроизвести» путь получения: что осматривалось, какие идентификаторы были, какое время, какая среда отображения, какие действия совершены. Это имеет первостепенное значение, потому что интернет-контент может выглядеть по-разному у пользователей (персонализация) и может быть подвергнут изменениям.

На использование ресурсов сети «Интернет» для получения криминалистически значимой информации непосредственно направлены так называемые электронно-технические следственные действия (контроль и запись переговоров, наложение ареста на почтово-телеграфные отправления, их осмотр и выемка, получение информации о соединениях между абонентами и (или) абонентскими устройствами[245]). Особенностью их производства выступает то, что

[245] См., например: Берова Д. М. Особенности использования компьютерной информации из сети «Интернет» при расследовании преступлений в Российской Федерации // Пробелы в российском законодательстве. 2020. № 2. С. 147–149 ; Организация расследования и тактика отдельных следственных действий по делам о преступлениях,

в отличие от других рассмотренных нами следственных действий следователь их не проводит, а только принимает решение и даже не может при них присутствовать (как это предусмотрено для производства судебной экспертизы). Всю техническую работу по получению необходимой информации выполняют иные субъекты, даже не являющиеся участниками уголовного судопроизводства. В настоящее время круг этих субъектов расширился, как и технические возможности по получению необходимых сведений. Очевидно, что уголовно-процессуальная норма не успевает за развитием информационных технологий. Регламентация законодателем указанных следственных действий и вынужденное совершенствование соответствующих норм УПК РФ (например, введение части 7 в ст. 185) не разрешают возникающих противоречий. В современном электронно-цифровом мире коммуникаций последние уже объединены в единую систему электронной связи. Нормы же закона о производстве перечисленных технических действий все еще регламентируют взаимоотношения с почтовыми службами, учреждениями кабельных телефонных и телеграфных сетей, предлагают порядок контроля и фиксации ограниченных способов коммуникаций.

Ряд ученых формулируют возможные пути преодоления указанных противоречий. Так, А. И. Зазулин считает необходимым исключить из ст. 185 УПК РФ часть 7, а дополнить этим положением ст. 186.1, назвав норму «Получение информации о соединениях между абонентами и (или) абонентскими устройствами, а также информации, содержащейся в сообщениях, передаваемых посредством сервисов электронной почты, обмена мгновенными сообщениями или иным подобным образом»[246]. Схожей позиции придерживается О. М. Ефремова, предлагающая расширить сферу следственного действия, предусмотренного статьей 186.1 УПК РФ, на правовые отношения между следователем и организаторами распространения информации в сети «Интернет», назвав законодательную новеллу следующим образом: «Статья 186.1. Получение

совершенных с использованием информационно-телекоммуникационных технологий / А. Б. Соколов, М. М. Горшков, А. А. Кузнецов [и др.]. Омск : Омская академия МВД России, 2023.

[246] См.: Зазулин А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : дис. … канд. юрид. наук. Екатеринбург, 2018. С. 247–249.

компьютерной информации у операторов связи и организаторов распространения информации в сети “Интернет”». Свое предложение она обосновывает тем, что в отличие от получения сведений о соединениях между абонентами и (или) абонентскими устройствами следователь запрашивает компьютерную информацию не только у организаций связи, но и у организаций, распространяющих информацию в сети «Интернет», а предмет технического запроса следователя у исполнителя и процессуальная основа получения компьютерной информации практически идентичны[247].

Довольно сложно согласиться с используемым О. М. Ефремовой столь широким термином «компьютерная информация» для указанных следственных действий, а также с включением в название статьи и соответствующего следственного действия того наименования субъектов получения информации, которым в настоящее время оперирует Федеральный закон «О связи». В частности, речь идет о понятии «оператор связи» и перечне лиц, обязанных предоставлять сведения, что в контексте уголовно-процессуального регулирования требует более узкой и специфичной интерпретации. При развитии технологий и соответствующем изменении их правового регулирования потребуется вновь менять название следственного действия, которое, на наш взгляд, должно носить универсальный, стабильный характер на долгие годы. В связи с этим нам импонирует позиция В. С. Черкасова, предложившего объединить обсуждаемые три следственных действия в одно — «контроль электросвязи». Однако исследователь констатирует, что в существующих технических и правовых условиях преждевременно удалять из УПК РФ статью 186.1 «Получение информации о соединениях между абонентами и (или) абонентскими устройствами», и предлагает исправить недостатки ее уголовно-процессуальной конструкции[248].

---

[247] См.: Ефремова О. М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий : автореф. дис. … канд. юрид. наук. С. 25–27.

[248] См.: Черкасов В. С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса. С. 154.

Пока названные изменения не приняты законодателем, сам следователь вынужден использовать интернет-ресурсы не самостоятельно, а опосредованно — через других уполномоченных субъектов. При этом затрачиваются значительные временны́е и организационные силы на оформление большого количества процессуальных документов для производства трех видов следственных действий, позволяющих получить электронную криминалистически значимую информацию.

Обращение к возможностям этих электронно-технических следственных действий также должно быть подчинено вышеуказанным принципам. При этом опосредованный характер производства отмеченных действий ставит перед правоприменителем дополнительную проблему, связанную с необходимостью изучения и познания процесса получения доказательственной информации. Для пояснения этого тезиса приведем типичный пример.

В рамках судебного следствия по уголовному делу о превышении должностных полномочий сторона защиты заявила несколько ходатайств об исключении из числа доказательств результатов биллинга телефона подсудимого, полученных в порядке ст. 186.1 УПК РФ. Основаниями признания доказательства недопустимым выступали результаты анализа соединений телефона обвиняемого, сопоставленные с другими сведениями о его местопребывании, которые вступали в противоречие с отдельными моментами обвинения. Для разрешения обозначенных защитой несоответствий судья вынужден был допросить не только специалиста, применявшего аппаратно-программный комплекс по определению местоположений абонента, но и представителей сотовых операторов, служб монтажа оборудования сотовой связи. Результатами допросов указанных специалистов об особенностях прохождения сигнала сотовой связи, его фиксации конкретным оборудованием, специфике определения искомой информации конкретным программным устройством и пр. заявленные ходатайства были разрешены без ущерба для обвинительного тезиса. Однако для этого потребовалось

провести несколько судебных заседаний, что затянуло судебное следствие на полтора месяца[249].

И это не единственный пример, когда правоприменителю, не обладающему специальными компьютерно-техническими знаниями, непонятно, каким образом получен результат следственного действия, требующего сложных манипуляций с программным обеспечением. Что касается судебных экспертиз, то строгая структура изложения экспертного заключения снимает эту проблему благодаря подробному описанию методов исследования и ссылкам на конкретные экспертные методики (83 % изученных нами заключений судебных экспертиз содержали такое описание). Если анализировать практику проведения осмотров, обысков, сопряженных с обнаружением и изъятием электронно-цифровой информации, а также электронно-технических следственных действий, то их протоколы зачастую не содержат описания порядка производимых специалистами действий (в 74 % изученных протоколов соответствующее описание отсутствовало).

Судебная перспектива признания надлежащим доказательством полученных из сети «Интернет» сведений зависит от того, насколько воспроизводимы условия их получения. Для этого в процессуальных документах должно быть подробно изложено: что осматривалось, где, когда, при каких настройках, с какими реквизитами источника. Минимальным стандартом фиксации в протоколе электронно-цифровой информации должно быть указание на:

— точную ссылку/URL или внутренний идентификатор объекта (ID поста, ID канала/аккаунта);

— дату и время фиксации (желательно с указанием часового пояса);

— условия доступа (публично/после входа; наличие/отсутствие авторизации);

— описание последовательности действий (что нажималось, что открывалось);

[249] См.: Уголовное дело № 1-3/2023 // Архив Реутовского гарнизонного военного суда за 2024 г.

— фиксацию релевантных метаданных (где они доступны без вмешательства).

Например, фиксация снимка экрана (скриншота) и его приложение к протоколу без URL/ID, а также без описания условий отображения легко оспариваются стороной защиты как «изображение неизвестного происхождения». Соблюдение принципов воспроизводимости и проверяемости снимает подобные возражения оппонентов.

## § 2. Особенности использования сети «Интернет» при производстве вербальных следственных действий

Использование современных информационно-телекоммуникационных технологий позволяет оптимизировать производство традиционных вербальных следственных действий. Влияние научно-технического прогресса и иных объективных внешних факторов неизбежно обусловливает необходимость модернизации тактики их проведения.

Внедрение дистанционных технологий производства следственных действий на стадии предварительного расследования, по аналогии с судебными стадиями, активно обсуждается в юридической литературе[250]. Глобальная пандемия и

[250] См.: Андреева О. И., Зайцев О. А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12. С. 57–61 ; Бушкевич Н. С. Перспективы развития уголовного процесса в условиях глобальной цифровизации белорусского общества // Совершенствование следственной деятельности в условиях информатизации : сборник материалов Международной научно-практической конференции (Минск, 12–13 апреля 2018 г.). Минск, 2018. С. 49–50 ; Марковичева Е. В. Перспективы развития электронного судопроизводства в Российской Федерации // Российское правосудие. 2017. № 3 (131). С. 88–95 ; Желтобрюхов С. П. О необходимости предоставления органу предварительного расследования возможности применения видео-конференц-связи на стадии досудебного производства // Российская юстиция. 2016. № 1. С. 62–64 ; Мазунин Я. М., Белова К. С. Особенности фиксации допроса, проводимого с использованием видеоконференцсвязи [Электронный ресурс] // Технологии XXI века в юриспруденции : материалы Четвертой международной научно-практической конференции (Екатеринбург, 20 мая 2022 г.) / отв. ред. Д. В. Бахтеев. Екатеринбург : Уральский государственный юридический университет имени В.Ф. Яковлева, 2022. С. 27–30. 1 CD-ROM ; Родивилина В. А. Некоторые вопросы применения видео-конференц-связи в досудебном производстве // Вестник Иркутского государственного технического университета. 2015. № 2 (97). С. 278–280 ; Сидорова К. С. Особенности производства допроса с использованием видеоконференцсвязи // Криминалистика: актуальные вопросы теории и практики : сборник материалов Международной научно-практической конференции, Ростов-на-Дону, 7 июня 2019 г. / отв. ред. В. В. Осяк. Ростов-н/Д. : Ростовский юридический институт МВД России, 2019. С. 193–199 ; Щерба С. П., Архипова Е. А. Применение видео-конференц-связи в уголовном судопроизводстве России и зарубежных стран: опыт, проблемы, перспективы : монография. М. : Юрлитинформ, 2016 и др.

вынужденная изоляция обусловили ускорение законодательных механизмов, что привело к принятию дополнений в уголовно-процессуальный закон, предусматривающих возможность проведения допроса, очной ставки и опознания путем использования систем видео-конференц-связи (ВКС) на стадии предварительного расследования (ст. 189.1 УПК РФ)[251].

Законодатель не стал определять процессуальных субъектов указанных следственных действий, обязывать следователя выносить соответствующее постановление, а также вывел за рамки регулирования вопросы места их производства, порядка межведомственного взаимодействия и удостоверения протокола. Это отчасти нивелировало дискуссии, существовавшие на момент разработки соответствующего законопроекта. Однако, несмотря на то, что возможность применения ВКС при допросе в российском уголовном процессе предусмотрена с 2011 г., накопленная правоприменительная практика уже обнажила ряд до сих пор не разрешенных проблем процессуального и тактического характера.

Одна из обсуждаемых в юридической литературе и на практике проблем — это отсутствие в УПК РФ определения ВКС, что, на наш взгляд, обусловило нормативное ограничение для применения ряда интернет-сервисов, т.к. в ст. 189.1 говорится только о применении систем ВКС, которыми имеют право пользоваться государственные органы. Между тем опрос следователей органов внутренних дел и Следственного комитета РФ свидетельствует о крайне редком применении ВКС при допросе именно по причине отсутствия в следственном органе оборудованных ведомственной защищенной системой ВКС специальных помещений либо из-за неудовлетворительного ее функционирования[252]. Как правило, такие системы и помещения наличествуют только в региональных управлениях следственных органов.

---

[251] Федеральный закон от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СПС «КонсультантПлюс».

[252] Результаты опроса, как и собственный практический опыт работы автора следователем, дают основание утверждать, что ведомственная телекоммуникационная сеть в органах полиции практически постоянно функционирует с техническими помехами, чаще всего выражающимися в зависании изображения либо регулярных кратковременных прерываниях трансляции.

На наш взгляд, следует согласиться с Н. Г. Шурухновым, С. П. Павловым, С. А. Грачевым и другими учеными, считающими, что не сто́ит ограничиваться ведомственными системами ВКС, т.к. подобное ограничение не только исключает выбор информационно-телекоммуникационных средств допроса, но и привязывает следователя к конкретному органу, лишая его территориальной и временно́й маневренности[253]. Необходимость оперативного реагирования на постоянно поступающую новую криминалистически значимую информацию обусловливает принятие неотложных тактических и процессуальных решений о производстве следственных действий, в том числе дополнительных допросов, очных ставок и предъявлений для опознания. Такая необходимость может возникнуть у следователя при производстве других следственных действий вне его служебного кабинета, и он должен иметь возможность со своего персонального компьютера установить ВКС непосредственно в месте своего нахождения. Существующее законодательное ограничение исключает возможность оперативного реагирования и требует затяжной организационной подготовки для сбора всех участников как минимум в двух местах, оборудованных ведомственными системами ВКС.

Естественно, основной аргумент противников такого подхода сводится к соблюдению режима конфиденциальности, обусловленного тайной предварительного расследования[254]. Однако при сегодняшнем стремительном развитии цифровизации никто не может гарантировать конфиденциальность любой системы, и степень защиты ведомственной телекоммуникационной сети не будет, вероятно, выше популярных интернет-мессенджеров. Судебная практика знает немало примеров, когда помимо легальных систем суды использовали для допросов и иные интернет-сервисы[255].

---

[253] См.: Шурухнов Н. Г. Правовые и информационно-технические процедуры производства допроса посредством систем видео-конференц-связи (анализ отдельных положений ст. 189.1 УПК РФ) // Российский следователь. 2022. № 7. С. 26–30 ; Грачев С. А. Проведение следственных действий с применением видео-конференц-связи: поправки внесены, эффективность под вопросом // Российский следователь. 2022. № 9. С. 18–22 ; Павлов С. П. Производство следственных действий с применением видео-конференц-связи // Молодой ученый. 2023. № 12 (459). С. 103–104.

[254] См.: Стельмах В. Ю. Порядок производства следственных действий по видео-конференц-связи // Российский судья. 2022. № 10. С. 25–29.

[255] См.: Шурухнов Н. Г. Указ. соч.

В связи с этим закономерно возникает вопрос о допустимости доказательств, полученных с помощью не ведомственных, а иных технологий связи. В этом случае представляется, что критерием допустимости должно выступать соблюдение установленной процессуальной формы и обеспечение неизменяемости аудиовидеопотока. Для минимизации рисков признания таких доказательств недопустимыми целесообразно использование исключительно отечественного программного обеспечения, сертифицированного в установленном порядке уполномоченными государственными органами.

Верховный Суд РФ с 2019 г. стал активно использовать проведение судебных заседаний с участием граждан с помощью веб-конференции, которая позволяет участвовать в процессе, находясь при этом в офисе или дома. «Для этого участникам процесса необходимо через личный кабинет заблаговременно до даты судебного заседания направить в суд соответствующее заявление и документы, а также пройти идентификацию и аутентификацию через портал государственных услуг. В случае удовлетворения судом такого заявления, участникам судебного заседания направляется в личный кабинет и на электронную почту гиперссылка на подключение к виртуальному залу судебного заседания Верховного Суда Российской Федерации. В назначенную дату судебного заседания участники судебного процесса подключаются к системе видео-конференц-связи с помощью личных средств современной техники и связи. Для подтверждения своей личности они авторизуются на портале государственных и муниципальных услуг, далее их личность и полномочия проверяются судом, после чего они допускаются к участию в судебном заседании»[256].

Представляется, что правовая позиция Верховного Суда РФ, выработанная применительно к судебным стадиям, должна найти дальнейшее нормативное закрепление при регламентации порядка организации и проведения вербальных следственных действий в досудебном производстве.

---

[256] Веб-конференция в Верховном Суде Российской Федерации [Электронный ресурс] // URL: https://vsrf.ru/press_center/news/28867/ (дата обращения: 12.12.2024).

В этой части отечественному законодателю можно использовать зарубежный опыт. В частности, в пункте 1 ч. 2 ст. 69 УПК Эстонской Республики предусмотрено проведение дистанционного допроса при помощи технических средств, в результате чего показания допрашиваемого лица непосредственно видны и слышны в прямой трансляции и ему можно задавать вопросы[257]. Сами технические средства, их виды или характер действий не указываются, их выбор оставляется на усмотрение следователя.

Таким образом, закон должен предусматривать процессуальную возможность применения интернет-технологий в ходе следственного действия, а уже установленные законодателем и апробированные практикой процессуальные средства проверки доказательств позволяют оценить их допустимость при получении таким дистанционным способом.

На наш взгляд, в этих целях в ст. 5 УПК РФ необходимо предусмотреть определение видео-конференц-связи. В качестве такового нам импонирует формулировка Д. С. Гриня, который предложил под ВКС понимать компьютерно-цифровую технологию, в установленных уголовно-процессуальным законом случаях и порядке обеспечивающую дистанционное аудиовизуальное взаимодействие в режиме реального времени нескольких абонентов — участников уголовного судопроизводства, с возможностью добавления к каналу связи дополнительных абонентов, имеющих уголовно-процессуальный статус, в целях обмена аудио- и видеоинформацией посредством обособленной телекоммуникационной сети либо с использованием закрытых каналов сети «Интернет»[258]. Использование такого определения на законодательном уровне позволит шире применять усмотрение следователя при принятии решения, по каким каналам связи целесообразно в конкретный момент провести дистанционное следственное действие. Таким образом, это повысит адаптивность следственной практики к ситуационной вариативности.

---

[257] См.: Уголовно-процессуальный кодекс Эстонской Республики (ред. от 08.01.2021) [Электронный ресурс] // URL: https://https://www.juristaitab.ee/ru/ugolovno-processualnyy-kodeks (дата обращения: 25.01.2025).

[258] См.: Гринь Д. С. Теоретическое и нормативное определение видео-конференц-связи в уголовном судопроизводстве // Юридическая наука. 2020. № 3. С. 82–85.

Еще одним дискуссионным вопросом использования систем ВКС является защищенность каналов передачи данных в контексте положений ст. 161 УПК РФ о недопустимости разглашения данных предварительного расследования. В результате несанкционированного вмешательства третьих лиц может не только прерваться связь, но и открыться доступ к конфиденциальной информации, обсуждаемой в ходе следственного действия.

Рассматривая вопросы защиты информации, передаваемой по каналам связи, некоторые исследователи допускают возможность ее передачи и по открытым, специально не защищенным каналам. Например, С. Б. Вепрев и В. Ю. Рогозин считают возможным использовать открытые каналы связи для передачи конфиденциальных сведений, но с применением методов стеганографического сокрытия самого факта передачи данных. В этом контексте стеганография предполагает, что передаваемый текст растворяется в сообщении большего объема с совершенно посторонним смыслом[259]. Вероятно, такой метод передачи информации может показаться эффективным и не ведущим к ее утрате.

Вместе с тем необходимо обеспечить как внешнюю, так и внутреннюю защиту каналов связи для недопущения перехвата информации, передаваемой в ходе видеозвонков. Современное программное обеспечение для аудио- и видеовызовов автоматически шифрует данные в процессе общения. Однако полноценная защита передаваемой информации должна поддерживаться и внутренней защитой самого технического устройства, с которого осуществляется видеозвонок. Это связано прежде всего с установкой антивирусного программного обеспечения и настройкой безопасности брандмауэра (файрвола) для недопущения перехвата контроля над сетевым экраном.

С учетом названных факторов защиты передаваемой информации перечень необходимых технических средств для производства такого следственного действия является минимальным:

---

[259] См.: Вепрев С. Б., Рогозин В. Ю. О возможности передачи служебной информации по открытым каналам связи // Расследование преступлений: проблемы и пути их решения. 2016. № 2. С. 123.

— ноутбук или планшетный компьютер со встроенным микрофоном и веб-камерой либо фронтальной камерой (на мобильном телефоне) с пропускной способностью канала связи, позволяющей отчетливо передавать изображение на экран. В связи с этим возможно установить видеосервер внутри локальной сети конкретного отдела полиции для совершения звонков посредством ВКС либо обеспечить таким доступом каждый рабочий компьютер следователя с выдачей персональных логина и пароля;

— подключение выбранного устройства к сети «Интернет» со скоростью, обеспечивающей четкое отображение человека на экране и распознаваемую передачу звука без каких-либо помех: камера должна обеспечивать четкое изображение, часто ориентируются на минимальное разрешение 1280 × 720 пикселей. Желательно, чтобы и по горизонтали, и по вертикали угол был не менее 60º. Это помогает, чтобы в кадре целиком помещалось лицо участника, и было удобно рассматривать мимику. Важно, чтобы изображение не было размытым, отсутствовали сильные искажения, шумы или артефакты — это критично для последующей оценки показаний[260];

— зарегистрированные учетные записи в используемом программном обеспечении.

Другая проблема, требующая осмысления, напротив, вытекает из чрезмерно широкого дозволения законодателя на применение следователем своего усмотрения при реализации положений ст. 189.1 УПК РФ. Отсутствие в указанной норме обязанности должностного лица выносить постановление, а также абстрактное условие ч. 2 («В случае необходимости…»), с одной стороны, уменьшает дублирующий бумажный документооборот и не ограничивает властные полномочия, с другой стороны, ставит дополнительную задачу по установлению пределов такого усмотрения. Как верно отмечено А. В. Волченко и Е. В. Лакеевой, такой подход законодателя «может вызвать необоснованное применение систем

[260]См.: Руденко А. В., Бондаренко Ю. А., Балугина Т. С. Организация допроса с использованием средств видео-конференц-связи на территории российской федерации // Общество: политика, экономика, право. 2022. № 8 (109). С. 36-42.

ВКС (например, допрос по ВКС свидетеля, проживающего только лишь на другом конце города, а не в ином регионе)»[261]. Широкое усмотрение следователя при применении ст. 189.1 УПК РФ в сочетании с технологиями искусственного интеллекта может привести к его профессиональному самоустранению из-за роботизации когнитивных функций допроса. Доступность дистанционного формата в совокупности с применением искусственного интеллекта может подтолкнуть следователя к делегированию ему ключевых задач — сбора характеризующего материала, планирования тактики допроса, в частности тактических приемов, и т.д. В результате следователь из активного тактика и аналитика трансформируется в пассивное лицо, которое лишь использует подсказки нейросети и формально заверяет подписью автоматически сгенерированный протокол. Подобное, по нашему мнению, является недопустимым, поскольку замена живого аналитического мышления алгоритмами искусственного интеллекта нарушит принцип непосредственности исследования доказательств, породит различные ошибки, а также нивелирует индивидуальный подход к личности и справедливую оценку обстоятельств дела.

На наш взгляд, правоприменителю целесообразно обозначить пределы его усмотрения посредством указания оснований для применения ВКС при производстве допроса, очной ставки и предъявления для опознания.

Как показывает анализ позиций ученых, а также материалов уголовных дел[262], к числу наиболее распространенных причин востребованности ВКС при производстве допроса относятся факторы, связанные с:

1) обеспечением разумного срока уголовного судопроизводства (49 %);

2) невозможностью прибытия лица (состояние здоровья, не позволяющее совершать переезды и перелеты, и др.) (92 %);

3) обеспечением безопасности допрашиваемого лица (100 %);

4) значительными материальными затратами (37 %);

---

[261] Волченко А. В., Лакеева Е. В. Возможности использования видео-конференц-связи при производстве следственных действий // Вестник Восточно-Сибирского института МВД России. 2022. № 4 (103). С. 123–133.

[262] Лишь в единичных случаях следователями использовались возможности ВКС при производстве допроса, в то время как потребность в применении данной системы присутствовала более чем в 57 % дел.

5) нахождением лица в местах лишения свободы или содержанием под стражей (84 %);

6) сохранением конфиденциальности допрашиваемого лица и факта его дистанционного сотрудничества со следствием (67 %).

Практически те же причины применения ВКС определены в уголовно-процессуальных кодексах других государств, например в УПК Казахстана и Республики Беларусь, где дополнительно выделяются случаи допроса малолетнего или несовершеннолетнего свидетеля[263].

С. Д. Долгинов указывает, что практически те же случаи имели место и в проекте федерального закона, предусматривающего возможность применения ВКС. Хотя они не вошли в обсуждаемую норму, по мнению ученого, их необходимо в ней закрепить. Им выделяются следующие случаи:

«1) при невозможности явки участника следственного (процессуального) действия в орган дознания или к следователю по состоянию здоровья;

2) при нахождении участника следственного (процессуального) действия на территории, значительно отдаленной от места нахождения инициатора проведения допроса или очной ставки;

3) обеспечение явки участника к следователю или выезд самого следователя к месту его нахождения сопряжены со значительными временными и материальными затратами;

4) при отсутствии возможности в отдаленных местностях пригласить своевременно адвоката;

5) при отсутствии возможности предварительно осуществить конвоирование из мест заключения осужденного, проходящего по делу свидетелем;

6) если невозможна явка участника следственного (процессуального) действия к следователю в связи со стихийным бедствием;

---

[263] См.: ст. 213 Уголовно-процессуального кодекса Республики Казахстан от 04.07.2014 № 231-V [Электронный ресурс] // URL: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 25.01.2025) ; ст. 224.1 Уголовно-процессуального кодекса Республики Беларусь от 16.06.1999 [Электронный ресурс] // URL: https://etalonline.by/document/?regnum=hk9900295 (дата обращения: 20.03.2026).

7) если в производстве следственного (процессуального) действия участвует несовершеннолетний потерпевший или свидетель;

8) в случае необходимости обеспечения безопасности лиц, участвующих в следственном действии»[264].

На наш взгляд, такое подробное деление оснований больше подходит для официальных комментариев к правовой норме, а в законе должны найти закрепление более общие формулировки. Кроме того, мы не можем в полной мере согласиться с выделением такого основания, как допрос несовершеннолетнего потерпевшего или свидетеля. Целесообразность его выделения ученые преимущественно связывают с необходимостью создания для участвующих в следственных действиях детей психологически комфортной обстановки. Например, по мнению О. С. Пашутиной и Д. В. Алымова, «использование видео-конференц-связи при производстве следственных действий с участием малолетних (несовершеннолетних) участников позволит им в психологически комфортной обстановке дать показания об известных обстоятельствах»[265]. Однако возникает вопрос: в чем сложность для следователя провести следственное действие в месте нахождения ребенка, где будет присутствовать психологически комфортная обстановка? При существующей процедуре применения ВКС только в специально оборудованных кабинетах следственных органов, вызывает большие сомнения то, что обстановка в другом оснащенном ВКС следственном кабинете будет более комфортна для малолетнего или несовершеннолетнего, чем кабинет следователя, в производстве которого находится уголовное дело.

В связи с изложенным предпочтительно согласиться с формулировкой дополнения ч. 1 ст. 189.1 УПК РФ перечнем оснований для производства дистанционных следственных действий, предложенных А. В. Волченко и Е. В. Лакеевой:

---

[264] См.: Долгинов С. Д. Технологии применения видеоконференцсвязи на предварительном следствии: проблемы сегодняшнего дня // Пермский юридический альманах. 2023. Вып. 6. С. 470–485.

[265] Пашутина О. С., Алымов Д. В. Очная ставка: проблемные аспекты уголовно-процессуального регулирования // Российский следователь. 2020. № 6. С. 13–16.

— невозможность непосредственного прибытия лица к месту расследования (рассмотрения) уголовного дела по состоянию здоровья или другим уважительным причинам;

— необходимость обеспечения безопасности лица;

— наличие причин, дающих основания полагать, что следственные действия будут затруднены или связаны с излишними затратами[266].

Такой вариант, на наш взгляд, более приемлем и должен найти закрепление в УПК РФ.

Изложенные тактико-процессуальные особенности обусловливают введение в тактику допроса с использованием ВКС принципа объективной обоснованности. Его суть заключается в том, что следователю необходимо тщательно анализировать и учитывать конкретные обстоятельства, которые делают обращение к ВКС технически и юридически необходимым в каждом конкретном случае.

Следующей проблемой, именно с криминалистических позиций, выступает ограниченность тактического арсенала при проведении допроса посредством ВКС.

Тактике допроса и очной ставки посвящено огромное количество работ ученых-криминалистов[267]. В большинстве этих трудов тактические приемы подразделяются в зависимости от следственной ситуации, от характеристик допрашиваемого лица, задач следственного действия, категории уголовного дела и т.д.

Естественно, при дистанционном (опосредованном экраном) допросе ряд традиционных тактических приемов имеют ограниченное действие. Так, приемы эмоционально-психологического воздействия, опосредованные экраном, не так эффективны, как при живом общении. Из-за отсутствия непосредственного

---

[266] См.: Волченко А. В., Лакеева Е. В. Указ. соч. С. 131.

[267] См.: Питерцев С. К., Степанов А. А. Тактические приемы допроса : учебное пособие. 4-е изд., перераб. СПб. : С.-Петерб. юрид. ин-т, 2006 ; Коновалов С. И., Моторин А. С Допрос в уголовном судопроизводстве: проблемы соотношения процессуальных и тактических аспектов : монография. Ростов-н/Д : Изд-во ДЮИ, 2008 ; Бочкарев М. В. Психологические основы тактики допроса подозреваемого и обвиняемого. Саратов : СЮИ МВД России, 2008 ; Бертовский Л. В. Допрос. Тактика и технологии. М. : Экзамен, 2015 ; Васильев А. Н., Карнеева Л. М. Тактика допроса при расследовании преступлений. М. : Юрид. лит., 1970 ; Доспулов Г. Г. Психология допроса на предварительном следствии. М. : Юрид. лит., 1976 ; Зайцева И. А. Процессуальные и тактические особенности допроса подозреваемого и обвиняемого, проводимого при участии защитника. М. : Юрлитинформ, 2006 ; Зорин Г. А. Руководство по тактике допроса. М. : Юрлитинформ, 2001, и др.

визуального и пространственного контакта следователю сложнее установить психологический контакт с допрашиваемым. В таких случаях становится труднореализуемым применение приемов поиска совпадающего интереса, проявления интереса к личности допрашиваемого, выявления положительных, способствующих общению, и отрицательных, препятствующих ему, качеств.

В условиях конфликтной ситуации допроса по ВКС проблематично применение приемов повышенного эмоционального воздействия, связанных с предъявлением неожиданной информации (таких как внезапность, инерция, создание эмоционального напряжения и пр.), т.к. у допрашиваемого всегда есть возможность создания паузы из-за заявления о некачественности звука или изображения, что еще раз свидетельствует о необходимости соблюдения технических условий, указанных выше (качество картинки, трафик и пр.). Кроме того, при дистанционном допросе теряют свою эффективность приемы использования индикаторов поведения, основанные на вербальных и невербальных признаках лжи. Как правило, настройка видеотрансляции ориентирована на общий план всей обстановки допроса для фиксации нахождения и поведения всех участников следственного действия. Это обусловливает удаленность камеры от допрашиваемого лица и, соответственно, проблематичность фиксации мимических реакций допрашиваемого на конкретные вопросы следователя. С другой стороны, обязательное ведение видеозаписи дает возможность следователю при ее последующем просмотре и увеличении изображения оценить ход проведенного по ВКС допроса, выявить не замеченные ранее поведенческие признаки и реакции на конкретные вопросы, а также с учетом этого спланировать дополнительный допрос и другие следственные действия.

Кроме того, целесообразно использование программы VibraImage, которая позволяет автоматизировать диагностику поведения допрашиваемого, его психоэмоционального и физиологического состояния по видеоизображению[268].

[268] Система контроля психоэмоционального состояния человека (версия VibraImage 7.0) [Электронный ресурс] // URL: http://www.elsys.ru/vibraimage.php (дата обращения: 04.09.2026).

Более того, на восприятие информации негативно влияют внешние технические факторы. Большая площадь кабинета и некорректное размещение микрофонов приводят к появлению эха, звуковым искажениям, которые важны, особенно для распознавания лжи. С целью минимизации этих рисков к подготовке и настройке ВКС сто́ит привлекать специалиста.

При существующем постоянном техническом развитии, полагаем, уже имеется возможность трансляции изображения общим и крупным планами с нескольких ракурсов. А в дальнейшем, как считают ученые, функцию оценки поведенческих признаков возьмет на себя искусственный интеллект, который в режиме реального времени будет считывать и оценивать вербальные и невербальные признаки лжи, а затем указывать на них допрашивающему[269], возможно, даже с предложением формулировок последующих вопросов, провоцирующих замеченные реакции или выясняющих причины их проявления.

В связи с изложенным следует рекомендовать при проведении допроса с использованием ВКС делать акцент на тактических приемах, активизирующих память, направленных на детализацию показаний, связанных с демонстрацией прямых доказательств, пресекающих ложь, содержащих логический анализ противоречий, и пр.[270] Это позволяет сформулировать специфический для проводимых по ВКС следственных действий принцип — рационального выбора тактических приемов.

Проблемными аспектами также отличается стадия фиксации следственных действий, проводимых посредством ВКС.

На первый взгляд законом четко определен порядок фиксации обсуждаемого дистанционного способа производства следственных действий. Однако выделение в качестве отдельного процессуального документа некой подписки порождает различные интерпретации в фиксации как на практике, так и в юридической

---

[269] См.: Зайцев О. А. Особенности уголовно-процессуального доказывания в условиях цифровизации // Журнал российского права. 2024. № 8. С. 93–112.

[270] См.: Белова К. С. Особенности применения тактических приемов в ходе допроса с использованием видеоконференц-связи // Юридическая наука и образование в эпоху искусственного интеллекта : сборник статей по материалам Международного научно-практического форума, г. Тюмень, 16–18 октября 2025 г. / отв. ред. Е. А. Вакорина. Тюмень : ТюмГУ-Press, 2025. С. 29–32.

литературе. Например, С. Д. Долгинов считает, что протокол, составляемый согласно ч. 3 ст. 189.1 УПК РФ следователем-инициатором, должен быть отсканирован и направлен по месту нахождения допрашиваемого по электронной почте на адрес следователя-организатора. Последнему необходимо распечатать документ, предоставить его для ознакомления участникам следственного действия, а сам факт ознакомления отразить в подписке. В то же время присланный по электронной почте и распечатанный протокол также должен быть подписан участниками, поскольку в итоге в материалах дела будет два протокола: один — составленный по месту нахождения следователя-инициатора без подписей допрошенных и участников следственного действия со стороны следователя-организатора, а другой — со всеми подписями, присланный инициатору следователем-организатором[271].

Полагаем, что подобные рекомендации вызваны существующей в практике тенденцией к излишней перестраховке из-за опасений возврата уголовного дела для устранения недостатков. Это подтверждается как результатами опроса следователей (84 %), так и изученными немногочисленными примерами допросов по ВКС. Между тем судебная практика исходит из презумпции добросовестности следователя, которую суд всегда может проверить в ходе разбирательства при непосредственном участии субъектов процесса. В данном контексте и законодатель предусмотрел подписку скорее как способ фиксации оригинальных подписей участников следственных действий. Их подлинность по оригиналам, а не по копиям при необходимости всегда можно дополнительно проверить экспертным путем.

Множественностью процессуальных и технических процедур отличаются рекомендации указанных авторов и по видеозаписи дистанционных следственных действий. С. Д. Долгинов полагает, что видеозапись обязан вести следователь-организатор, который затем направляет ее инициатору вместе с подпиской и иными материалами.

---

[271] См.: Долгинов С. Д. Указ. соч.

Схожие рекомендации давались учеными и до введения ст. 189.1 УПК РФ. Например, А. А. Поддубняк и И. С. Евдокимова поясняли, что протокол допроса посредством ВКС составляется и оглашается с соблюдением всех требований действующего УПК РФ должностным лицом следственного органа или органа дознания по месту нахождения допрашиваемого лица. Затем следователю, в производстве которого находится уголовное дело, направляется протокол, который он удостоверяет своей подписью[272].

А. В. Волченко и Е. В. Лакеева отмечают неопределенность подписки (сколько в ней должно быть подписей и за что именно нужно расписываться?)[273]. Однако законом четко определено, что разъясняются права, обязанности, ответственность и порядок следственного действия, а также должна быть запись об оглашении протокола. Соответственно, о разъяснении этих положений участвующие лица должны поставить подписи, удостоверяющие их понимание сути происходящего. Единственное, в норме нет указания на удостоверение личности допрашиваемого. Но это требование вытекает из общих положений производства любого следственного действия (ч. 5 ст. 164 УПК РФ), а значит, нет необходимости его дублировать в специальной норме.

По мнению А. В. Волченко и Е. В. Лакеевой, следует приобщать копию паспорта допрашиваемого лица в подтверждение удостоверения его личности. Но по видеосвязи следователь-инициатор и так видит и допрашиваемого, и его паспорт, дополнительно это видит следователь-организатор, и оба вписывают паспортные данные в протокол и подписку.

Они также рекомендуют передавать составленный протокол по ведомственной сети для ознакомления и подписания. Однако в отличие от С. Д. Долгинова авторы предлагают оформлять и пересылать единый документ.

Впрочем, возможности современного программного обеспечения для видеозвонков позволяют осуществлять запись непосредственно внутри самой

---

[272] См.: Поддубняк А. А., Евдокимова И. С. Допрос свидетеля посредством видео-конференц-связи на стадии предварительного расследования как новелла российского законодательства // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2018. Т. 4 (70). № 3. С. 160.

[273] См.: Волченко А. В., Лакеева Е. В. Указ. соч.

программы. При этом будет записываться экран в режиме мультиэкрана[274], где каждое окно через веб-камеру транслирует лицо участника процесса в настраиваемом масштабе. Поскольку запись ведется программными средствами, она может содержать достоверные геолокационные данные GPS-позиционирования о местонахождении участников. Такая видеозапись и станет приложением к протоколу допроса. Для помощи в настройке технического оборудования и контроля процесса записи полагаем целесообразным привлекать специалиста.

Полагаем: данный вариант применим в повседневных реалиях, однако он может повлечь временны́е затраты, что существенно снизит оперативность получения информации. Поэтому в условиях стремительной цифровизации всех направлений государственной деятельности считаем допустимым предложить еще один вариант фиксации — получение доказательства в форме видеозаписи допроса как обязательное и юридически значимое дополнение к текстовому протоколу[275].

Тема видеопротоколирования стала весьма актуальной в научной юридической среде в последнее время. Профессор О. А. Зайцев считает, что в сегодняшних условиях «необходимо изменить существующие представления об уголовно-процессуальной форме, которая вступает в противоречие с современными способами получения (фиксации, хранения, предоставления, объективизации и визуализации) доказательственной информации. Электронный документ, аудиозапись, видеозапись, а также сведения из баз данных должны иметь равнозначный статус с протоколом, представляющим по сути письменную форму документооборота. Действующие жесткие требования оформительского характера к доказательствам создают препятствия для внедрения цифровизации в уголовное судопроизводство. В связи с этим следует пересмотреть правила допустимости

---

[274] Мультиэкран — система одновременного вывода на экран изображений нескольких участников видеоконференции.

[275] Более подробно данный вопрос рассмотрен в работах: Сидорова К. С. Особенности производства допроса с использованием видео-конференц-связи // Криминалистика: актуальные вопросы теории и практики : материалы международной научно-практической конференции. Ростов-н/Д : РЮИ МВД России, 2019. С. 193–199 ; Мазунин Я. М., Сидорова К. С. Организационные особенности производства допроса с использованием видеоконференц-связи // Технологии XXI века в юриспруденции : материалы Всероссийской научно-практической конференции. Екатеринбург : УрГЮУ, 2019. С. 98–102.

доказательств, содержащих электронную информацию или электронные носители информации, в пользу технических гарантий верифицируемости и полезности доказательства»[276].

П. П. Ищенко отмечает, что «в современных условиях протокол, как способ фиксации хода и результатов следственных действий, может быть с успехом заменен, к примеру, видеозаписью, защищенной от изменений криптографической защитой, сохраняемой и приобщаемой к электронному уголовному делу в цифровом формате»[277]. С. Д. Шестакова и С. Л. Виноградова также признают возможным сократить число звеньев передачи доказательственной информации, рассматривая материалы аудио- и видеозаписи в качестве альтернативы протоколу следственного действия[278]. С этой позицией солидарен Д. А. Гришин, предлагающий внести в уголовно-процессуальный закон изменения, которые позволят следователю или дознавателю не составлять протокол, если ход и результаты следственного действия фиксируются с помощью видеозаписи[279].

Ряд ученых, соглашаясь с указанной позицией, всё же считают необходимым сохранить основной способ фиксации в бумажной или электронной форме. Например, О. В. Качалова, разделяя приведенные точки зрения, отмечает: при использовании исключительно видео- или аудиопротокола быстрый поиск и получение конкретной «точечной» информации на электронных носителях (в отличие от визуального просмотра обычного протокола) могут быть затруднены. В связи с этим исследователь указывает на необходимость постепенного перехода к видеопротоколированию следственных действий с временным сохранением дублирующей традиционной системы. Она также предлагает зафиксировать в законе обязательное составление краткого протокола-справки, отражающего

---

[276] Зайцев О. А. Указ. соч.

[277] Ищенко П. П. Следственные действия в условиях цифровизации уголовного судопроизводства // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1 (35). С. 30–42.

[278] См.: Шестакова С. Д., Виноградова С. Л. О новых подходах к процессуальному значению материалов аудио- и видеозаписи, применяемых при производстве следственных действий, в условиях цифровизации // Уголовное судопроизводство России: проблемы и перспективы развития : материалы всероссийской научно-практической конференции / под ред. Э. К. Кутуева. СПб., 2020. С. 393–396.

[279] См.: Гришин Д. А. Цифровизация досудебного уголовного судопроизводства // Вестник Томского государственного университета. 2020. № 455. С. 208–215.

наиболее существенные обстоятельства следственного действия[280]. Схожий способ преодоления этого недостатка предлагает С. В. Зуев. Он считает нужным дублировать видеопротокол краткой справкой с указанием точного времени (минут и секунд) фиксации ключевых обстоятельств на видеозаписи[281]. Аналогичной позиции придерживается и С. А. Рябчиков, аргументируя это тем, что большинство следственных действий динамичны и проходят в быстро меняющейся обстановке. В таких условиях, по его мнению, введение видеопротоколирования взамен классического протокола становится особенно актуальным, если заменить последний кратким описанием. Такой подход позволит следователю полностью сконцентрироваться на самом процессе и обеспечит объективность его проведения, не отвлекая на заполнение «бумажного протокола». Для решения проблемы ознакомления с материалами автор предлагает внести изменения в уголовно-процессуальный закон, внедрив видеопротоколирование и обязательную справку о проведенном следственном действии[282].

Х. Х. Рамалданов считает, что проблему длительного ознакомления с видеопротоколом и поиска в нем нужной информации может решить система тайм-кодов (последовательность числовых кодов, генерируемых с регулярными интервалами системой синхронизации времени). Для этого при видеосъемке следственного действия необходимо указывать временны́е метки и названия эпизодов. Однако следует обратить внимание, что ученый предлагает ввести видеопротокол лишь для таких следственных действий, как следственный эксперимент, обыск и проверка показаний на месте[283].

---

[280] См.: Качалова О. В. Уголовно-процессуальные проблемы информатизации современного уголовного судопроизводства // Российское правосудие. 2019. № 2. С. 93–100.

[281] См.: Зуев С. В. Цифровое видеопротоколирование следственных действий: возможности и перспективы // Ученые записки : сборник научных трудов, Оренбург, 14–15 ноября 2019 г. Оренбург : РПК «Полиарт», 2020. С. 7–10.

[282] См.: Рябчиков С. А. Видеопротоколирование как средство уголовно-процессуального доказывания // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24. № 2. С. 56–62.

[283] См.: Рамалданов Х. Х. Видеопротоколирование как основа цифровизации уголовного судопроизводства // Юристъ-Правоведъ. 2022. № 4 (103). С. 86–92.

Другая группа ученых (А. Д. Назаров, Д. А. Руденко, А. Б. Судницын), ссылаясь на схожую позицию профессора Л. Н. Масленниковой[284] и опыт Республики Казахстан, настаивает на сохранении протокола как формы фиксации, однако видит необходимость его трансформации из бумажной плоскости в электронную. «Избранный подход к необходимости сохранения протокольной формы с одновременной ее трансформацией в электронную плоскость в большей мере отвечает целям уголовного судопроизводства, поскольку такая удостоверительная технология обусловливает достаточно высокую степень достоверности и адекватности соответствующих познавательных результатов для дальнейшего использования»[285].

Мы солидарны с последней точкой зрения, тем более что современное программное обеспечение позволяет на заключительной стадии фиксации следственного действия преобразовывать видеосъемку в текстовый файл. Программы-транскрибаторы сегодня способны наиболее точно передавать содержание речи с видеозаписи[286]. Однако ввиду разного тембра голосов, их силы звучания, внятности произношения и прочих речевых особенностей преобразованные тексты содержат ошибки (как правило, в знаках препинания, написании числительных, правильности передачи падежей и склонений) и требуют редактирования, что также занимает достаточно много времени. Полагаем, что при стремительном развитии цифровых технологий программы транскрибации станут более совершенными. До этого момента при переходе на электронную форму протокола, дублирующую видеопротокол, необходимо будет указывать, что текст описательной части следственного действия воспроизведен с видеозаписи посредством конкретной программы-транскрибатора без редактирования и может

---

[284] См.: Масленникова Л. Н. Концептуальный подход к построению уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 10 (74). С. 52–65.

[285] Руденко Д. А. Деформализация уголовного судопроизводства в контексте развития цифровых технологий : выпускная квалификационная работа. СПб. : СПбГУ, 2024. С. 102–104.

[286] См.: Кузьмин Д. Как превратить голос в текст: тестируем 6 сервисов для расшифровки [Электронный ресурс] // URL: https://journal.tinkoff.ru/list/voice-txt/ (дата обращения: 12.01.2025) ; Перевод аудио в текст: ТОП 5 программ для распознавания речи [Электронный ресурс] // URL: https://eks-libris.ru/blog/perevod-audio-v-tekst-top-5-programm-dlya-raspoznavaniya-rechi/ (дата обращения: 12.01.2026) и др.

содержать грамматические ошибки. Соответственно, при оценке достоверности и допустимости полученной в ходе следственного действия доказательственной информации исследованию подлежит видеопротокол, а поиск конкретных данных в нем облегчает электронный протокол с трансформированной в текст видеозаписью.

Рассуждая о тактике проведения такого вербального следственного действия, как очная ставка, следует отметить, что необходимость ее проведения с использованием ВКС может быть обоснована в первую очередь трудностью сбора всех участников в одном месте в определенное время. В связи с этим верно отмечают А. Г. Маркелов и М. А. Нефедов: «С учетом транспортной доступности места проведения предварительного расследования, мест проживания участников очной ставки, их целенаправленного уклонения от явки на допрос, необходимости одновременного доставления их к месту производства следственного действия, а также невозможности лишения свободы передвижения одного из участников очной ставки до прибытия другого участника к месту ее производства, имеющаяся в распоряжении следователя мера процессуального принуждения в виде принудительного привода в этом случае практически нереализуема»[287], что также дает основание для проведения очной ставки в дистанционном режиме посредством ВКС.

С. А. Сумин предлагает рассматривать в качестве оснований для проведения очной ставки с использованием ВКС значительную территориальную удаленность ранее допрошенных лиц, в показаниях которых имеются существенные противоречия. Кроме того, он считает, что при необходимости обеспечения конфиденциальности и безопасности лица, дающего показания (а также его близких родственников, родственников и близких лиц), следователь (дознаватель) вправе провести очную ставку с применением ВКС, в том числе с созданием

[287] Маркелов А. Г., Нефедов М. А. Особенности проведения отдельных следственных действий с использованием инновационных технологий по уголовным делам в сфере экономики // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 1. С. 137.

аудиовизуальных помех, исключающих визуальное наблюдение защищаемого лица другими участниками следственного действия[288].

Безусловно, все выделенные выше основания дистанционного проведения допроса применимы и к очной ставке. Однако целесообразно согласиться с позициями данных ученых и признать, что необходимость проведения очной ставки в режиме ВКС также должна быть обоснованной и разумной, чтобы не повлечь за собой ограничение или нарушение прав и законных интересов участников следственных действий.

Итак, если имеется основание для проведения очной ставки с использованием ВКС, а техническое оснащение позволяет выполнить данное следственное действие, то, как и при допросе, его необходимо осуществлять путем направления поручения в ОВД по месту нахождения участника очной ставки. Если участников несколько и они находятся в разных населенных пунктах, то количество поручений определяется этим фактором. Сама процедура очной ставки должна быть аналогична порядку, описанному выше применительно к допросу.

Не менее результативным следственным действием является предъявление для опознания (ст. 193 УПК РФ). Данное следственное действие также возможно производить с использованием ВКС по основаниям и в порядке, изложенным выше. Более того, как верно отмечает А. И. Гаевой, современные возможности сети «Интернет» позволяют передавать видеоизображение людей и предметов (документов) без искажения и с очень высокой скоростью[289].

В качестве опознаваемых объектов законом предусмотрены лицо, предмет, а также труп. В связи с этим следует отметить: даже если имеется одно из оснований для производства данного следственного действия с использованием ВКС, объективная возможность его проведения существует не всегда. Предметы могут

---

[288] См.: Сумин С. А. Применение систем видео-конференц-связи при допросе защищаемых территориально удаленных лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности // Вестник Воронежского института МВД России. 2011. № 3. С. 71.

[289] См.: Гаевой А. И. Современные информационно-телекоммуникационные технологии как средство повышения эффективности следственных действий: проблемы и перспективы их использования в уголовном судопроизводстве России // Информационная безопасность регионов. 2007. № 1. С. 68.

быть слишком больших или, напротив, крайне малых размеров, из-за чего продемонстрировать их в натуральную величину через экран довольно сложно, что затрудняет опознание. Опознание трупа во многом базируется на исследовании специфических признаков, которые невозможно передать посредством видеосвязи (едва заметные шрамы, родинки, татуировки, скрытые элементами одежды, или текстура кожных покровов).

Помимо этого, согласно ч. 8 ст. 193 УПК РФ в целях обеспечения безопасности опознающего предъявление лица для опознания по решению следователя может быть проведено в условиях, исключающих визуальное наблюдение опознающего опознаваемым. Полагаем, что для такого вида опознания необходимо отдельное помещение, исключающее возможность наблюдения из него за иными лицами. В связи с этим целесообразно отметить, что функции современного программного обеспечения позволяют предъявлять объект для опознания в режиме онлайн и в условиях, исключающих визуальное наблюдение опознающего опознаваемым, — например, путем целенаправленного выключения веб-камеры одного из участников видеозвонка или создания помех.

Исходя из этого следует сказать, что предъявление для опознания посредством ВКС целесообразно производить, когда имеется необходимость исключить визуальное наблюдение опознающего опознаваемым при условии, что объект возможно идентифицировать в таком режиме. Задействование ВКС при производстве других следственных действий на стадии предварительного расследования действующим УПК РФ не регламентируется, но и запрет на ее использование отсутствует. Более того, в соответствии с ч. 6 ст. 164 УПК РФ при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. Полагаем, что данная норма может относиться и к частному случаю использования ВКС в ходе проведения иных следственных действий (преимущественно направленных на получение вербальной информации) с соблюдением общих правил их производства. Как верно отмечает М. А. Михайлов, «уже существующие, многократно проверенные “классические” следственные

действия являются надежной платформой для придания легитимности результатам использования технических новшеств эпохи информационных технологий»[290].

Таким образом, проведенное исследование позволяет сделать вывод о том, что интеграция систем видео-конференц-связи в досудебное производство должна осуществляться при строгом сохранении единства уголовно-процессуальной формы.

## Выводы по третьей главе

1. Специфика тактики реализации невербальных следственных действий, проводимых с использованием сети «Интернет», сводится к решению следующих тактических задач: поисково-познавательных и обеспечительных.

2. Поисково-познавательная задача будет решаться с целью использования сети «Интернет» для отыскания, фиксации и получения криминалистически значимой информации, которая за счет процессуальной формы следственного действия преобразуется в доказательственную. Решение обеспечительной задачи позволяет в ходе следственного действия с помощью сети «Интернет» обеспечить удаленный доступ к источнику криминалистически значимой информации, ориентироваться на местности, дистанционно проводить следственное действие, а также анализировать его результаты.

3. Определены принципы использования интернет-ресурсов при производстве отдельных следственных действий: юридической адресности, двухпоточности действий, тактической оперативности, технологической верифицируемости, технического обеспечения минимизации потери информации, обеспечения допустимости полученных доказательств, воспроизводимости и проверяемости, объективной обоснованности, рационального выбора тактических приемов.

---

[290] Михайлов М. А. Будущее следственных действий в эпоху информационных технологий: эволюция или революция // Уголовное производство: процессуальная теория и криминалистическая практика : материалы VI Международной научно-практической конференции. Симферополь : Ариал, 2018. С. 72–74.

4. Предлагаются тактические особенности дистанционного обыска в рамках алгоритма по:

1) установлению IP-адреса и физического адреса (MAC-адрес);

2) изучению данных браузера, использовавшегося интересующим следствие лицом для доступа к ресурсам;

3) преодолению систем ограничения доступа к компьютерной информации;

4) анализу истории просмотра веб-страниц и закладок в браузере;

5) исследованию электронной почты;

6) проверке инструментов синхронизации данных;

7) выявлению способов анонимизации;

8) применению программ поиска файлов;

9) восстановлению недавно удаленной информации;

10) копированию обнаруженных и подлежащих изъятию сведений;

11) описанию предпринятых в ходе обыска попыток уничтожить исследуемую информацию и принятых мер по их пресечению.

В зависимости от вида расследуемой преступной деятельности и отражающей ее в компьютерных сетях криминалистически значимой информации предложенный алгоритм должен быть конкретизирован с указанием содержания искомых сведений.

5. Для обеспечения возможности применения различных интернет-сервисов в процессе ВКС, а не только ведомственных технических систем, указанных в ч. 1 ст. 189.1 УПК РФ, целесообразно закрепить в ст. 5 Кодекса дефиницию видео-конференц-связи. Отсутствие в данном определении законодательных ограничений по выбору технических средств позволит шире использовать усмотрение следователя при принятии решения о том, по каким каналам связи наиболее эффективно в конкретный момент провести дистанционное следственное действие.

6. Пределы усмотрения правоприменителя, на наш взгляд, необходимо обозначить посредством нормативного закрепления в уголовно-процессуальном законе оснований для применения ВКС при производстве допроса, очной ставки и

предъявления для опознания: 1) невозможность непосредственной явки лица к месту расследования (рассмотрения) уголовного дела по состоянию здоровья или иным уважительным причинам; 2) необходимость обеспечения безопасности участника; 3) наличие обстоятельств, дающих основания полагать, что следственные действия без ВКС будут затруднены либо связаны с излишними затратами.

7. Обязательная видеозапись позволяет следователю при ее последующем просмотре и увеличении изображения оценить ход проведенного по ВКС допроса, выявить не замеченные ранее поведенческие признаки или реакции на конкретные вопросы и с учетом этого спланировать дополнительный допрос либо иные следственные действия.

8. Рекомендуется при проведении дистанционного допроса делать акцент на тактических приемах, активизирующих память, направленных на детализацию показаний, связанных с демонстрацией прямых доказательств, пресекающих ложь, а также содержащих логический анализ противоречий, и т.д.

9. Предъявление для опознания посредством ВКС целесообразно производить при необходимости исключить визуальное наблюдение опознающего опознаваемым и при условии, что данный объект возможно идентифицировать в таком режиме.

10. Задействование ВКС при производстве других следственных действий на стадии предварительного расследования действующим УПК не регламентируется, но и запрет на ее использование отсутствует. Более того, согласно ч. 6 ст. 164 УПК РФ при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных доказательств. Полагаем, что данная норма может относиться и к частному случаю использования ВКС в ходе проведения иных следственных действий (преимущественно направленных на получение вербальной информации) с соблюдением общих правил их производства.

# ЗАКЛЮЧЕНИЕ

Разрешение поставленных в диссертационном исследовании задач позволило прийти к следующим выводам.

1. Информационно-телекоммуникационная сеть «Интернет» в силу своего содержания и специфического устройства является самостоятельным объектом познания криминалистической науки — элементом функциональной стороны криминальной и антикриминальной деятельности. Это обусловливает необходимость включения в предметную область криминалистики закономерностей не только применения цифровых технологий при подготовке, совершении и сокрытии преступлений, но и возникновения и отражения следов преступления в Сети, выявления, фиксации, изъятия и использования данных интернет-ресурсов для получения криминалистически значимых сведений о преступной деятельности и ее участниках.

2. Применительно к деятельности следователя, осуществляющего расследование конкретного посягательства, выявлено, что не вся сеть «Интернет» выступает объектом познания, а те ее ресурсы, которые могут содержать криминалистически значимую информацию по находящемуся в его производстве уголовному делу.

3. Для сферы уголовного судопроизводства ресурс сети «Интернет» можно определить как информационную технологию, содержащую системно обусловленную, принципиально достижимую с помощью программно-аппаратных средств, потребляемую информацию, способствующую эффективному решению задач расследования преступлений.

4. Предложена классификация ресурсов сети «Интернет», имеющая значение для отыскания, передачи, получения и использования криминалистически значимой информации: по характеру данных (контент, метаданные, сетевые и операторские сведения); по правовому режиму доступа и способу легитимного получения сведений (открытого, условно-открытого, закрытого доступа,

анонимизированного/скрытого сегмента); по субъекту владения и управления ресурсом (государственные и муниципальные ресурсы, коммерческие платформы и сервисы, инфраструктурные субъекты интернет-среды, пользовательские (социальные) ресурсы); по функциональному назначению в расследовании (поисково-навигационные, идентификационно-атрибутивные, коммуникационные, транзакционно-финансовые, геоинформационные и мультимедийные, мониторингово-аналитические, профилактические).

5. Задачи предварительного расследования выводятся из нормативных установлений, которые предписано обязательно выполнять следователю по каждому уголовному делу. С криминалистических позиций деятельность следователя связана с выбором определенных наиболее эффективных и, главное, целесообразных способов действий. Соответственно, его действия должны предусматривать возможность гибко реализовать тактический замысел и достичь целей расследования в пределах, допустимых законом и полномочиями. Тем самым задачи процессуальные дополняются задачами тактическими, а точнее, трансформируются в них.

6. Анализ выделенных признаков тактической задачи показывает, что они имеют обязательную трехчленную структуру:

1) ситуационный фактор, определяемый исходной информацией;

2) требование изменения этого фактора конкретным тактическим способом воздействия;

3) направленность на достижение цели расследования.

7. В зависимости от обусловленного следственной ситуацией содержания и объема разрешаемых вопросов, основываясь на уголовно-процессуальной классификации задач предварительного расследования, можно выделить по содержательному критерию следующие тактические задачи расследования преступлений:

1) раскрытие преступления;

2) установление лица, потерпевшего от преступления, в том числе личности трупа;

3) задержание лица, совершившего преступление;

4) проверка алиби лиц, возможно причастных к преступлению;

5) изобличение лица, совершившего преступление;

6) розыск обвиняемого, иных лиц, предметов и документов, имеющих значение для дела;

7) выявление и пресечение противодействия расследованию;

8) обеспечение безопасности участников расследования;

9) обеспечение возмещения причиненного преступлением вреда, имущественных взысканий и конфискации;

10) выявление и устранение причин и условий, способствовавших совершению преступления.

8. Разделение ресурсов сети «Интернет» на источник информации и средство ее получения образует организационные формы использования этих ресурсов при раскрытии и расследовании преступлений, причем их выбор обусловливается задачами по обнаружению, фиксации, изъятию, исследованию и использованию криминалистически значимой информации, решаемыми посредством тактических комбинаций и операций.

Направления использования ресурсов глобальной Сети задаются тактическими задачами, разрешаемыми посредством криминалистических операций и комбинаций.

9. Ресурсы сети «Интернет» во всех выделенных по содержанию решаемых тактических задач криминалистических операциях могут быть реализованы в двух организационных формах:

‘— как источник криминалистически значимой информации;

— как средство выявления, фиксации и передачи криминалистически значимой информации.

10. Раскрыта сущность тактической операции по использованию ресурсов сети «Интернет» при расследовании преступлений как комплексного криминалистического средства планомерного решения локальных задач расследования, связанных с поиском, фиксацией, проверкой и процессуальным

закреплением информации, содержащейся на интернет-ресурсах, хранящейся на программно-аппаратных средствах. Ее специфика обусловливается динамичностью трансформации цифровых объектов, многообразием источников криминалистически значимой информации, рисками утраты данных и ошибок в процессе их интерпретации.

11. Направления использования ресурсов сети «Интернет» представлены криминалистическими операциями (комбинациями) по:

— установлению информации о посягательстве, позволяющей квалифицировать его как преступление, и совершившем его лице;

— установлению лица, потерпевшего от преступления, в том числе личности трупа;

— изучению личности лица, совершившего преступление;

— задержанию лица, совершившего преступление;

— проверке алиби лиц, возможно причастных к преступлению;

— изобличению лица, совершившего преступление;

— привлечению подозреваемого (обвиняемого) к сотрудничеству путем заключения досудебного соглашения о сотрудничестве;

— розыску обвиняемого, иных лиц, предметов и документов, имеющих значение для уголовного дела;

— выявлению и пресечению противодействия расследованию;

— обеспечению безопасности участников расследования;

— обеспечению возмещения причиненного преступлением вреда, имущественных взысканий и конфискации;

— выявлению и устранению причин и условий, способствовавших совершению преступления.

12. Использование сети «Интернет» как источника криминалистически значимой информации в целях установления события (или его отдельных элементов) преступления или неизвестных эпизодов преступной деятельности возможно в двух направлениях:

— для установления латентного (зачастую совершаемого с использованием сети «Интернет») посягательства (или его эпизодов/элементов);

— для получения дополнительной криминалистически значимой информации по очевидным преступлениям.

13. В первом направлении обращение к Сети необходимо, как правило, оперативным путем с привлечением специалистов для анализа «Даркнета» и зашифрованных мессенджеров. Акцент следует делать на ключевых субъектах: администраторе сайта, лице, размещающем противоправный контент, и потребителе (заказчике) этого контента. Здесь следует также выделить два вектора оперативной и процессуальной работы: 1) от сайта или 2) от потребителя (заказчика).

По первому вектору предлагается в рамках оперативного эксперимента создание копий известных криминальных сайтов либо самостоятельных сайтов — торговых площадок для реализации криминальных товаров и услуг — с дальнейшим отслеживанием заказа и доставки или внедрением компьютерного червя при нематериальном информационном заказе в рамках контролируемой поставки.

По второму вектору при поиске от потребителя (заказчика) рекомендуется использовать информацию провайдера о подключении к входной ноде, сопоставление времени выхода в «Даркнет», подключения к входной ноде и появления определенного преступного результата.

14. Второе направление получения криминалистически значимой информации по очевидным преступлениям представляет интерес в плане поиска информации, размещаемой на новостных сайтах, популярных развлекательных порталах, стриминговых сервисах и в мессенджерах.

15. Имеющиеся научные и практические разработки в области традиционной криминалистической идентификации не в полной мере позволяют осуществлять идентификацию человека, представленного в сети «Интернет», посредством идентификаторов. Это обусловливает необходимость установления идентификаторов пользователя сети «Интернет» и их принадлежности

техническому устройству, которое применяло физическое лицо при подготовке, совершении и сокрытии преступления, т.е. идентификации данного лица.

16. Идентификатор пользователя сети «Интернет» — это присваиваемая сетевому подключению или задаваемая пользователем уникальная комбинация символов, позволяющая в процессе раскрытия и расследования преступлений выделять конкретное лицо или оконечное оборудование из неопределенного круга, устанавливать устойчивую связь между виртуальным образом и реальным субъектом, а также документировать факты присутствия и выполнения отдельных операций в информационно-телекоммуникационной сети «Интернет».

17. Руководствуясь определением идентификатора пользователя, спецификой функционирования, целесообразно разделить перечисленные идентификаторы (IP-адрес, доменное, сетевое имена, простая электронная подпись) на две группы:

— «невидимый» идентификатор — IP-адрес;

— «видимые» идентификаторы — доменное, сетевое имена пользователя, простая электронная подпись.

18. При установлении провайдера связи по IP-адресу и его географическому положению возможно использовать интернет-ресурсы, однако требуется проверять такую неофициальную информацию процессуальными (направление запроса в адрес соответствующего провайдера) и непроцессуальными (проверка таких сведений на нескольких сайтах) способами. Ответы на запросы от провайдеров связи необходимо осматривать и приобщать в качестве иного документа согласно УПК РФ.

19. При исследовании видов IP-адресов было выявлено, что как по статическому, так и по динамическому IP-адресу действительно возможно идентифицировать физическое лицо. При этом необходимо выполнить комплекс следственных, процессуальных и непроцессуальных, действий и оперативно-разыскных мероприятий в подтверждение того, что IP-адрес использовало конкретное физическое лицо, осуществляя доступ в сеть «Интернет» при помощи

технического устройства, и задействовать в расследовании готовое и проверенное доказательство.

20. Исследование таких «видимых» идентификаторов пользователя, как доменное, сетевое имена пользователя, электронная подпись в расследовании преступления позволяет определить техническое устройство, с которого осуществлялся доступ в сеть «Интернет» с такими идентификаторами, а также физическое лицо, которое могло его использовать.

21. Сведения о значении того или иного сетевого имени пользователя в рамках расследуемого преступления возможно установить следователю самостоятельно на основе изучения общедоступных источников, руководствуясь криминалистическими познаниями, путем назначения лингвистической экспертизы, если получена переписка пользователя, путем допроса специалиста в области лингвистики.

22. Идентификация пользователей сети «Интернет» по электронной подписи позволит осуществить привязку каждого аккаунта пользователя к конкретному абонентскому номеру, что в целом поспособствует органам предварительного расследования в верной идентификации пользователя по первоначальной информации и в установлении всех обстоятельств, подлежащих доказыванию по уголовному делу.

23. Специфика тактики реализации невербальных следственных действий с использованием сети «Интернет» сводится к решению следующих тактических задач: поисково-познавательных и обеспечительных. Поисково-познавательная задача будет решаться с целью использования сети «Интернет» для отыскания, фиксации и получения криминалистически значимой информации, которая за счет процессуальной формы проводимого действия преобразуется в доказательственную. Решение обеспечительной задачи позволяет в ходе следственного действия с помощью сети «Интернет» реализовать возможности обеспечения удаленного доступа к источнику криминалистически значимой информации, ориентирования на местности, дистанционного производства следственного действия, анализа результатов следственного действия.

24. Определены принципы использования интернет-ресурсов при производстве отдельных следственных действий: юридической адресности, двухпоточности действий, тактической оперативности, технологической верифицируемости, технического обеспечения минимизации потери информации, воспроизводимости и проверяемости, объективной обоснованности, рационального выбора тактических приемов.

С опорой на указанные принципы сформулирована система практико-ориентированных рекомендаций по тактике отдельных следственных действий.

25. Предлагаются тактические особенности дистанционного обыска в рамках алгоритма по:

1) установлению IP-адреса и физического адреса (MAC-адреса);

2) изучению данных браузера, использовавшегося интересующим следствие лицом в доступе к ресурсам;

3) преодолению средств ограничения доступа к компьютерной информации;

4) изучению информации об истории просмотра веб-страниц и закладок в браузере;

5) изучению электронной почты;

6) исследованию средств синхронизации данных;

7) выявлению средств анонимизации;

8) применению средств поиска файлов;

9) восстановлению недавно удаленной информации;

10) копированию обнаруженной и подлежащей изъятию информации;

11) описанию предпринятых в ходе обыска попыток уничтожить исследуемую информацию и принятых мер.

В зависимости от вида расследуемой преступной деятельности и отражающей ее в компьютерных сетях криминалистически значимой информации предложенный алгоритм должен быть конкретизирован с указанием содержания искомых сведений.

26. Для реализации возможности применения различных интернет-сервисов в процессе ВКС, а не только ведомственных технических систем согласно ч. 1

ст. 189.1 УПК РФ, целесообразно в ст. 5 Кодекса предусмотреть дефиницию видео-конференц-связи. Отсутствие в данном определении законодательных ограничений по выбору технических средств позволит шире использовать усмотрение следователя при принятии решения о том, по каким каналам связи наиболее эффективно в конкретный момент провести дистанционное следственное действие.

27. Пределы усмотрения правоприменителя, на наш взгляд, целесообразно обозначить посредством указания в уголовно-процессуальном законе оснований к использованию ВКС для производства допроса, очной ставки и предъявления для опознания: 1) невозможность непосредственного прибытия лица к месту расследования (рассмотрения) уголовного дела по состоянию здоровья или другим уважительным причинам; 2) необходимость обеспечения безопасности лица; 3) наличие причин, дающих основания полагать, что следственные действия будут затруднены или связаны с излишними затратами.

28. Обязательное ведение видеозаписи дает возможность следователю при ее последующем просмотре и увеличении изображения оценить ход проведенного по ВКС допроса, выявить не замеченные поведенческие признаки и реакции на конкретные вопросы и, с учетом этого, спланировать дополнительный допрос и другие следственные действия.

29. Рекомендуется при подготовке к дистанционному допросу делать акцент на тактических приемах, активизирующих память, направленных на детализацию показаний, связанных с демонстрацией прямых доказательств, пресекающих ложь, содержащих логический анализ противоречий, и пр. Это позволяет сформулировать специфический для проводимых по ВКС следственных действий принцип — рационального выбора тактических приемов.

30. Задействование ВКС при производстве других следственных действий на стадии предварительного расследования действующим УПК не регламентируется, но и запрет на нее отсутствует. Более того, в соответствии с ч. 6 ст. 164 Кодекса при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступления и вещественных

доказательств. Предполагаем, что данная норма может относиться и к частному случаю использования ВКС в ходе проведения других следственных действий (преимущественно направленных на получение вербальной информации) с соблюдением общих правил их производства.

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

## 1. Нормативные правовые акты

### *1.1. Российские нормативные правовые акты, законопроекты*

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 ; тест, включающий новые субъекты Российской Федерации) [Электронный ресурс] // Официальный интернет-портал правовой информации. — Режим доступа: http://www.pravo.gov.ru. 06.10.2022.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства Российской Федерации. — 2001. — № 52 (ч. I). — Ст. 4921.

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — Ст. 3448.

5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. — 2011. — № 15. — Ст. 2036.

6. Федеральный закон от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. — 2022. — № 1 (ч. 1). — Ст. 12.

7. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. — 1995. — № 33. — Ст. 3349.

8. Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Собрание законодательства Российской Федерации. — 2008. — № 52. — Ст. 6228.

9. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. — 2003. — № 28. — Ст. 2895.

10. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. — 2011. — № 15. — Ст. 1909.

11. Федеральный закон от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. — 2021. — № 52. — Ст. 7737.

12. Федеральный закон от 14.02.2009 № 22-ФЗ «О навигационной деятельности» // Собрание законодательства Российской Федерацию. — 2009. — № 7. — Ст. 790.

13. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства Российской Федерации. — 2024. — № 20. — Ст. 2584.

14. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации. — 2019. — № 41. — Ст. 5700.

15. Распоряжение Правительства РФ от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // СПС «Гарант».

16. Постановление Правительства РФ от 28.11.2011 № 977 «О Федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной

форме"» // Собрание законодательства Российской Федерации. — 2011. — № 49. — Ст. 7273.

17. Постановление Правительства РФ от 14.09.2012 № 928 «О базовых государственных информационных ресурсах» // Собрание законодательства Российской Федерации. — 2012. — № 39. — Ст. 5273.

18. Постановление Правительства РФ от 12.08.2014 № 801 «О внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства Российской Федерации. — 2014. — № 33. — Ст. 4613.

19. Постановление Правительства РФ от 31.07.2014 № 759 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети "Интернет" информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети "Интернет" и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации» // Собрание законодательства Российской Федерации. — 2014. — № 32. — Ст. 4516.

20. Постановление Правительства РФ от 03.06.2019 № 710 (ред. от 17.08.2021) «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» // Собрание законодательства Российской Федерации. — 2019. — № 23. — Ст. 2963 ; 2021. — № 34. — Ст. 6223.

21. Законопроект № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» [Электронный ресурс] // Режим доступа: https://sozd.duma.gov.ru/bill/747513-7.

22. ГОСТ Р 7.0.107–2022 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу.

Библиотечно-информационная деятельность. Термины и определения». — М. : Стандартинформ, 2022. — 48 с.

23. ГОСТ Р 52872–2019 «Интернет-ресурсы и мобильные приложения. Доступность для пользователей с инвалидностью и других лиц с ограничениями жизнедеятельности». — М. : Стандартинформ, 2019. — 30 с.

24. ГОСТ Р 53632–2009 «Показатели качества услуг доступа в Интернет. Общие требования». — М. : Стандартинформ, 2009. — 12 с.

25. Информационный бюллетень Межпарламентской ассамблеи государств — участников Содружества Независимых Государств. — 2011. — № 51. — 398 с.

### 1.2. Зарубежные нормативные правовые акты

26. Уголовно-процессуальный кодекс Республики Беларусь от 16.07.1999 № 295-З [Электронный ресурс] // Режим доступа: https://etalonline.by/document/?regnum=hk9900295.

27. Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 № 231-V [Электронный ресурс] // Режим доступа: https://adilet.zan.kz/rus/docs/K1400000231.

28. Уголовно-процессуальный кодекс Эстонской Республики (ред. от 08.01.2021) [Электронный ресурс] // Режим доступа: https://www.juristaitab.ee/sites.

## 2. Материалы следственной и судебной практики

29. Определение Конституционного Суда РФ от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации» // СПС «Гарант».

30. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных путем неправомерного доступа к компьютерной информации или посредством использования электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет")» // Российская газета. — 28.12.2022. — № 293.

31. Уголовное дело № 1-333/2023 // Архив Красногорского городского суда Московской области.

32. Уголовное дело № 1-541/2023 // Архив Одинцовского городского суда Московской области.

33. Уголовное дело № 1-3/2023 // Архив Реутовского гарнизонного военного суда за 2024 г.

34. Материалы уголовного дела № 1-22/2013 // Архив Тюменского районного суда Тюменской области за 2013 г.

35. Приговор Вахитовского районного суда г. Казани от 18.07.2023 № 1-198/2023 по делу № 1-198/2023 [Электронный ресурс] // Режим доступа: https://sudact.ru/regular/doc/HoDtGgBkPkQu/.

36. Приговор Курганского городского суда от 04.02.2024 № 1-24/2023 по делу № 1-24/2023 [Электронный ресурс] // Режим доступа: https://sudact.ru/regular/doc/mwKQW3OWCEb5/.

37. Приговор Волжского городского суда Волгоградской области от 24.10.2016 по делу № 1-998/2016 [Электронный ресурс] // РосПравосудие. — Режим доступа: https://rospravosudie.com/court-volzhskij-gorodskoj-sud-volgogradskaya-oblast-s/act-535499180/.

38. Приговор Железнодорожного районного суда г. Улан-Удэ (Республика Бурятия) от 22.10.2025 по делу № 1-529/2025 [Электронный ресурс] // Режим доступа: https://sudact.ru/regular/doc/1RecpDC2GD6W/.

39. Приговор Иркутского районного суда № 1-19/2024 от 23.09.2024 // по делу № 1-19-2024 [Электронный ресурс]. Режим доступа: https://sudact.ru/regular/doc/IMfH34xgGRLK/.

40. Приговор Кировского районного суда г. Самары от 26.11.2012 по делу № 1-967/2012 [Электронный ресурс] // РосПравосудие. — Режим доступа: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-samary-samarskaya-oblast-s/act-416627668/.

41. Приговор Московского районного суда г. Чебоксары Чувашской Республики от 04.03.2016 по делу № 1-69/2016 [Электронный ресурс] // РосПравосудие. — Режим доступа: https://rospravosudie.com/court-moskovskij-rajonnyj-sud-g-cheboksary-chuvashskaya-respublika-s/act-524172066/.

42. Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа — Югры от 30.06.2015 по делу № 1-777/2015 [Электронный ресурс] // РосПравосудие. — Режим доступа: https://rospravosudie.com/court-nizhnevartovskij-gorodskoj-sud-xanty-mansijskij-avtonomnyj-okrug-s/act-495724621/.

43. Приговор Новочебоксарского городского суда Чувашской Республики от 27.11.2025 по делу № 1-314/2025 [Электронный ресурс] // Режим доступа: https://sudact.ru.

44. Приговор Щелковского городского суда Московской области от 09.11.2025 по делу № 1-567/2025 [Электронный ресурс] // Режим доступа: https://sudact.ru.

45. Приговор Якутского городского суда Республики Саха (Якутия) от 19.01.2018 по делу № 1-41/2018 [Электронный ресурс] // РосПравосудие. — Режим доступа: https://rospravosudie.com/court-yakutskij-gorodskoj-sud-respublika-saxa-yakutiya-s/act-579805767/.

46. Приговор Ханты-Мансийского районного суда, Ханты-Мансийского автономного округа-Югра от 01.02.2017 № 1-4/2017 1-451/2015 1-53/2016 по делу № 1-4/2017 [Электронный ресурс] // Режим доступа: https://sudact.ru/regular/doc/pUINI7jb9aLV/.

47. Приговор Железнодорожного городского суда Московской области от 04.12.2025 № 1-328/2025 по делу № 1-328/2025 [Электронный ресурс] // Режим доступа: https://sudact.ru/regular/doc/C3ewRvSJYB1X/.

48. Уголовное дело № 176709 (г. Екатеринбург) по обвинению Ф. в совершении преступления, предусмотренного частью 1 ст. 273 УК РФ.

## 3. Монографии, учебники, учебные пособия

49. Акиев, А. Р. Тактика следственного осмотра и исследования цифровой информации средств телекоммуникации и Интернета : учеб.-практ. пособие / А. Р. Акиев, К. И. Сотников. — СПб. : Санкт-Петербургский университет МВД России, 2023. — 68 с.

50. Бабакова, М. А. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий : монография / М. А. Бабакова, В. В. Степанов. — М. : Юрлитинформ, 2014. — 256 с.

51. Балакшин, В. С. Развитие информационных технологий в уголовном судопроизводстве / В. С. Балакшин, В. Б. Вехов, В. Н. Григорьев [и др.]. — М. : Юрлитинформ, 2018. — 320 с.

52. Бачило, И. Л. Информационное право : учебник для вузов / И. Л. Бачило. — 5-е изд., перераб. и доп. — М.: Юрайт, 2026. — 419 с.

53. Белкин, Р. С. Курс криминалистики : в 3 т. / Р. С. Белкин. Т. 3 : Криминалистические средства, приемы и рекомендации. — М. : Юристъ, 1997. — 400 с.

54. Белкин, Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории / Р. С. Белкин. — М. : Юрид. лит., 1987. — 320 с.

55. Белкин Р. С. Курс криминалистики / Р. С. Белкин. 3-е изд., доп. — М. : Юнити-Дана : Закон и право, 2001. — 837 с.

56. Бертовский, Л. В. Допрос. Тактика и технологии / Л. В. Бертовский. — М. : Экзамен, 2015. — 304 с.

57. Вандышев, В. А. Раскрытие преступлений, совершенных в условиях неочевидности / В. А. Вандышев, В. Я. Робозеров. — Л. : Изд-во ЛГУ, 1990. — 140 с.

58. Варданян, А. В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А. В. Варданян, Е. В. Никитина. — М. : Юрлитинформ, 2007. — 320 с.

59. Васильев, А. Н. Тактика допроса / А. Н. Васильев, Л. М. Карнеева. — М., 1970. — 120 с.

60. Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки / В. Б. Вехов. — Волгоград : ВА МВД России, 2008. — 404 с.

61. Гаврилин, Ю. В. Криминалистика в понятиях и терминах : учеб. пособие / Ю. В. Гаврилин, А. В. Головин, И. В. Тишутина. — М., 2006. — 384 с.

62. Голицына, И. Н. Мировые информационные ресурсы : учеб.-метод. пособие / И. Н. Голицына. — Казань : Казанский университет, 2014. — 52 с.

63. Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. — Киев : ТИД ДС, 2002. — 630 с.

64. Драпкин, Л. Я. Криминалистика : учебник / Л. Я. Драпкин, В. Н. Корагодин. — 2-е изд. — М., 2011. — 450 с.

65. Жарова, А. К. Право и информационные конфликты в информационно-телекоммуникационной сфере : монография / А. К. Жарова. — М. : Янус-К, 2016. — 248 с.

66. Жбанков, В. А. Криминалистические средства и методы установления лиц, совершивших преступления / В. А. Жбанков, Г. Н. Меглицкий. — М., 1993. — 180 с.

67. Зорин, Г. А. Теоретические основы криминалистики / Г. А. Зорин. — Минск : Амалфея, 2000. — 350 с.

68. Зорин, Г. А. Руководство по тактике допроса / Г. А. Зорин. — М.: Юрлитинформ, 2001. — 319 с.

69. Кирсанов, З. И. Криминалистические учения в механизме преступления и его расследовании / З. И. Кирсанов. — М., 2004. — 32 с.

70. Костылева, Г. В. Руководство для следователя по осмотру места происшествия / Г. В. Костылева, Н. Е. Муженская. — М., 2010. — 210 с.

71. Криминалистика : учебник для юридических вузов / под ред. В. А. Образцова. — М.: Юристъ, 1997. — 760 с.

72. Криминалистика. Углубленный курс / под общ. ред. А. Г. Филиппова. — М., 2012. — 480 с.

73. Курс криминалистики. Общая часть / отв. ред. В. Е. Корноухов. — М., 2000. — 512 с.

74. Кустов, А. М. Теоретические основы криминалистического учения о механизме преступления / А. М. Кустов. — М., 1997. — 124 с.

75. Макаренко, И. А. Личность несовершеннолетнего обвиняемого как объект криминалистического исследования / И. А. Макаренко. — М. : Юрлитинформ, 2006. — 352 с.

76. Малыхина, Н. И. Криминалистические методы и средства установления личности в процессе расследования преступлений / Н. И. Малыхина, Г. И. Поврезнюк. — М. : Юрлитинформ, 2005. — 366 с.

77. Мещеряков, В. А. Теоретические основы механизма следообразования в цифровой криминалистике : монография / В. А. Мещеряков. — М. : Проспект, 2022. — 176 с.

78. Образцов, В. А. Выявление и изобличение преступника : учеб. пособие / В. А. Образцов. — М. : Юристъ, 1997. — 336 с.

79. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. — М. : Норма, Инфра-М, 2018. — 352 с.

80. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 2-е изд. — СПб. : Питер, 2005. — 928 с.

81. Организация расследования и тактика отдельных следственных действий по делам о преступлениях, совершенных с использованием информационно-

телекоммуникационных технологий / А. Б. Соколов, М. М. Горшков, А. А. Кузнецов [и др.]. — Омск : Омская академия МВД России, 2023. — 164 с.

82. Питерцев, С. К. Тактические приемы допроса : учеб. пособие / С. К. Питерцев, А. А. Степанов. — 4-е изд., перераб. — СПб., 2006. — 56 с.

83. Понятие, классификация и структура тактических операций в расследовании преступлений : науч.-практ. пособие / под ред. Н. Ю. Пономаренко. — Белгород, 2017. — 120 с.

84. Развитие информационных технологий в уголовном судопроизводстве / В. С. Балакшин, В. Б. Вехов, В. Н. Григорьев [и др.] ; отв. ред. С. В. Зуев. — М. : Юрлитинформ, 2018. — 248 с.

85. Робачевский, А. М. Интернет изнутри: Экосистема глобальной Сети / А. М. Робачевский. — М. : Альпина Паблишер, 2015. — 480 с.

86. Россинская, Е. Р. Криминалистическая теория и практика в условиях цифровизации : монография / Е. Р. Россинская. — М. : Норма, Инфра-М, 2025. — 320 с.

87. Россинская, Е. Р. Настольная книга судьи: судебная экспертиза / Е. Р. Россинская, Е. И. Галяшина. — М. : Проспект, 2012. — 480 с.

88. Руденко, Д. А. Деформализация уголовного судопроизводства в контексте развития цифровых технологий: выпускная квалификационная работа. — Аспирантура СПБГУ, 2024.

89. Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учеб. пособие / Е. А. Русскевич. — М. : Инфра-М, 2024. — 160 с.

90. Рыжаков, А. П. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / А. П. Рыжаков. — М. : Гарант-сервис-университет, 2014. — 1200 с.

91. Словарь русского языка : в 4 т. / РАН, Ин-т лингвистич. исследований ; под ред. А. П. Евгеньевой. — 4-е изд., стер. — М. : Рус. яз. ; Полиграфресурсы, 1999.

92. Судницын, А. Б. Задачи предварительного расследования: правовая природа, система, проблемы реализации и пути совершенствования : монография / А. Б. Судницын. — Красноярск : СибЮИ МВД России, 2019. — 210 с.

93. Сурмин, Ю. П. Теория систем и системный анализ : учеб. пособие / Ю. П. Сурмин. — Киев : МАУП, 2003. — 368 с.

94. Цифровая криминалистика : учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — М. : Юрайт, 2024. — 450 с.

95. Щерба, С. П. Применение видео-конференц-связи в уголовном судопроизводстве России и зарубежных стран: опыт, проблемы, перспективы : монография / С. П. Щерба, Е. А. Архипова. — М. : Юрлитинформ, 2016. — 216 с.

96. Яблоков, Н. П. Криминалистика : практикум / Н. П. Яблоков. — М. : Юристъ, 2004. — 640 с.

97. IT-справочник следователя / под ред. докт. юрид. наук С. В. Зуева. — М. : Юрлитинформ, 2019. — 420 с.

98. Mukasey, M. B. Electronic Crime Scene Investigation : A Guide for First Responders. 2nd ed. / M. B. Mukasey, J. L. Sedgwick, D. W. Hagy. — U.S. Department of Justice, 2008. — 63 p.

## 4. Статьи

99. Авчиева, Д. Т. Системные связи термина «Никнейм» / Д. Т. Авчиева // Гуманитарные науки и образование. — 2015. — № 4. — С. 103–106.

100. Азаров, М. С. Доменные имена в структуре гражданского и информационного права / М. С. Азаров // Информационное право. — 2010. — № 2. — С. 11–18.

101. Айвазова, О. В. К вопросу о сущности понятия «раскрытие преступления» в контексте норм действующего законодательства /

О. В. Айвазова // Криминалистика: вчера, сегодня, завтра. — 2020. — № 2 (14). — С. 19–27.

102. Андреева, О. И. Российский уголовный процесс в эпоху коронавируса: вызовы времени / О. И. Андреева, О. В. Качалова // Вестник Томского государственного университета. Право. — 2020. — № 36. — С. 5–15.

103. Андреева, О. И. Перспективы ведения российского уголовного судопроизводства в электронном формате / О. И. Андреева, О. А. Зайцев // Уголовная юстиция. — 2018. — № 12. — С. 57–61.

104. Анешева, А. Т. К вопросу о возможностях использования информационно-телекоммуникационной сети «Интернет» в организации раскрытия и расследования преступлений / А. Т. Анешева, К. С. Сидорова // Пенитенциарная система и общество: опыт взаимодействия : сборник материалов V Международной научно-практической конференции, Пермь, 4–6 апреля 2018 г. / сост. В. А. Овченков. — Пермь : ФКОУ ВО Пермский институт ФСИН России, 2018. — С. 206–208.

105. Анешева, А. Т. Проверка сообщения о совершении преступления, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ / А. Т. Анешева, К. С. Сидорова // Сборник материалов криминалистических чтений. — 2017. — № 14. — С. 6–8.

106. Аникина, Т. В. Имя собственное в интернет-коммуникации / Т. В. Аникина // Известия Уральского государственного университета. Серия 1, Проблемы образования, науки и культуры. — 2010. — № 2. — С. 71–76.

107. Архипов, В. В. Открытая концепция регулирования Интернета вещей / В. В. Архипов, В. Б. Наумов, Г. А. Пчелинцев, Я. А. Чирко // Информационное право. — 2016. — № 2. — С. 18–25.

108. Аубакирова, А. А. Возможности использования Интернета при расследовании и профилактике преступлений / А. А. Аубакирова // Информатизация и информационная безопасность правоохранительных органов. — М. : Академия управления МВД России, 2008. — С. 338–343.

109. Ахмедшин, Р. Л. Поисковые следственные действия в системе следственных действий: криминалистический аспект / Р. Л. Ахмедшин // Вестник Томского государственного университета. 2015. — № 399. — С. 160–166.

110. Балкунова, А. С. Ценностные составляющие концепта «Я» языковой личности интернет-пространства / А. С. Балкунова // Ценности и смыслы. — 2012. — № 1. — С. 99–105.

111. Белова, К. С. Направления использования ресурсов сети «Интернет» при решении задач расследования преступлений / К. С. Белова // Российский следователь. — 2026. — № 1. — С. 2–6.

112. Белова, К. С. Особенности применения тактических приемов в ходе допроса с использованием видео-конференц-связи / К. С. Белова // Юридическая наука и образование в эпоху искусственного интеллекта : сборник статей по материалам Международного научно-практического форума, г. Тюмень, 16–18 октября 2025 г. / Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Школа права и управления ; науч. ред. С. С. Зенин ; отв. ред. Е. А. Вакорина. — Тюмень : ТюмГУ-Press, 2025. — 352 с.

113. Белова, К. С. Понятие и виды ресурсов сети Интернет, обращение к которым возможно в процессе расследования преступлений / К. С. Белова // Эксперт-криминалист. — 2026. — № 1. — С. 26–29.

114. Белова, К. С. Сеть Интернет как объект изучения криминалистической науки / К. С. Белова // Известия Юго-Западного государственного университета. Серия «История и право». — 2024. — Т. 14. — № 5. — С. 105–114.

115. Белова, К. С. Тактическая операция по использованию ресурсов сети «Интернет» при расследовании преступлений [Электронный ресурс] / К. С. Белова // Шикановские криминалистические чтения: криминалистическое и судебно-экспертное обеспечение расследования и раскрытия преступлений : материалы ежегод. Всерос. науч.-практ. конф. молодых исследователей, Иркутск, 17 дек. 2025 г. / отв. ред. Д. А. Степаненко. — Иркутск : Изд. дом БГУ, 2026. — С. 5–9. — Режим доступа: http://lib-catalog.bgu.ru.

116. Белова, К. С. Использование ресурсов сети «Интернет» в решении задач следственного осмотра / К. С. Белова // Правовой альманах. — 2025. — № 8 (48). — С. 7–13.

117. Бердичевский, Ф. Ю. О предмете и понятийном аппарате криминалистики / Ф. Ю. Бердичевский // Вопросы борьбы с преступностью. — 1976. — Вып. 24. — С. 131–149.

118. Берестова, Т. Ф. Информационное ресурсоведение как новое научное направление: постановка проблемы / Т. Ф. Берестова // Научно-техническая информация. Серия 1, Организация и методика информационной работы. — 2015. — № 7. — С. 1–9.

119. Берова, Д. М. Особенности использования компьютерной информации из сети «Интернет» при расследовании преступлений в Российской Федерации / Д. М. Берова // Пробелы в российском законодательстве. — 2020. — № 2. — С. 147–149.

120. Бушкевич, Н. С. Перспективы развития уголовного процесса в условиях глобальной цифровизации белорусского общества / Н. С. Бушкевич // Совершенствование следственной деятельности в условиях информатизации : сб. материалов Междунар. науч.-практ. конф., Минск, 12–13 апр. 2018 г. — Минск, 2018. — С. 49–50.

121. Быстров, А. К. Доменное имя и связанные с ним объекты / А. К. Быстров // Современное право. — 2014. — № 5. — С. 58–61.

122. Бушкевич Н.С. Перспективы развития уголовного процесса в условиях глобальной цифровизации белорусского общества // Совершенствование следственной деятельности в условиях информатизации : сб. материалов Междунар. науч.-практ. конф. — Минск, 2018. — С. 49–50.

123. Вепрев, С. Б. О возможности передачи служебной информации по открытым каналам связи / С. Б. Вепрев, В. Ю. Рогозин // Расследование преступлений: проблемы и пути их решения. — 2016. — № 2. — С. 123–128.

124. Вехов, В. Б. «Электронная криминалистика»: понятие и система / В. Б. Вехов // Криминалистика: актуальные вопросы теории и практики : сборник

трудов участников Междунар. науч.-практ. конф. — Ростов н/Д. : Ростовский юридический институт МВД России, 2017. — С. 40–46.

125. Вехов, В. Б. Электронные следы в системе криминалистики / В. Б. Вехов, Б. П. Смагоринский, С. А. Ковалев // Судебная экспертиза. — 2016. — № 2. — С. 10–19.

126. Вехов, В. Б. К вопросу криминалистического исследования анонимайзеров / В. Б Вехов, М. А. Ульянова // Актуальные научные исследования в современном мире. — 2018. — № 7-3. — С. 54-57.

127. Виноградова, О. П. Типичные следственные ситуации первоначального этапа расследования преступлений, совершаемые с использованием сети Интернет, в отношении несовершеннолетних / О. П. Виноградова // Научный вестник ОрЮИ МВД России им. В.В. Лукьянова. — 2025. — № 1 (102). — С. 169–179.

128. Волченко, А. В. Возможности использования видео-конференц-связи при производстве следственных действий / А. В. Волченко, Е. В. Лакеева // Вестник Восточно-Сибирского института МВД России. — 2022. — № 4 (103). — С. 123–133.

129. Волынский, А. Ф. Эффективность как принцип организации предварительного расследования преступлений / А. Ф. Волынский // Вестник Московского университета МВД России. — 2016. — № 4. — С. 27–32.

130. Галяутдинов, Р. Р. Документы, зафиксированные в электронном виде: особенности процессуальной и криминалистической оценки / Р. Р. Галяутдинов // Тенденции развития науки и образования. — 2023. — № 96-5. — С. 62–64.

131. Гаврилин, Ю. В. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах / Ю. В. Гаврилин, А. А. Балашова // Криминалистика: вчера, сегодня, завтра. — 2020. — № 1 (13). — С. 129–137.

132. Гаевой, А. И. Современные информационно-телекоммуникационные технологии как средство повышения эффективности следственных действий: проблемы и перспективы их использования в уголовном судопроизводстве

России / А. И. Гаевой // Информационная безопасность регионов. — 2007. — № 1. — С. 65–70.

133. Гайдин, А. И. Использование информационных ресурсов Интернет в расследовании преступлений / А. И. Гайдин // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : материалы Всерос. науч.-практ. конф. — Орел : Орловский юридический институт им. В.В. Лукьянова, 2016. — С. 89–90.

134. Гольцов, С. Е. Особенности расследования преступлений, совершаемых с применением средств анонимизации в сети Интернет и мобильной связи / С. Е. Гольцов // Теория и практика общественного развития. — 2023. — № 5. — С. 165–169.

135. Гончарова, Е. А. Использование сети Интернет в раскрытии и расследовании преступлений / Е. А. Гончарова // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки». — 2009. — Т. 22. — № 1. — С. 310–315.

136. Горбанев, В. М. Личностные характеристики преступников, совершающих мошенничества, связанные с использованием средств сотовой связи / В. М. Горбанев, А. К. Щербаченко, И. С. Бардадым // Юристъ-правоведъ. — 2017. — № 2. — С. 44–47.

137. Грановский, Г. Л. Понятие и основные положения теории решения криминалистических задач / Г. Л. Грановский // Современное состояние и перспективы развития традиционных методов криминалистических экспертиз : сб. науч. тр. — М. : Юрид. лит., 1987. — С. 5–18.

138. Гришин, Д. А. Цифровизация досудебного уголовного судопроизводства / Д. А. Гришин // Вестник Томского государственного университета. — 2020. — № 455. — С. 208–215.

139. Гринь, Д. С. Теоретическое и нормативное определение видео-конференц-связи в уголовном судопроизводстве / Д. С. Гринь // Юридическая наука : науч.-практ. журн. — 2020. — № 3. — С. 82–85.

140. Дёмин, К. Е. О перспективах исследования электронных документов как объектов судебной экспертизы / К. Е. Дёмин // Вестник экономической безопасности. — 2016. — № 4. — С. 33-37.

141. Дёмин, К. Е. Электронные документы как носители / К. Е. Дёмин // Совершенствование деятельности органов предварительного расследования и экспертно-криминалистических подразделений на современном этапе развития России : сборник научных статей. — Ставрополь : Секвойя, 2018. — С. 59–64.

142. Добринская, Д. Е. Киберпространство: территория современной жизни / Д. Е. Добринская // Вестник Московского университета. Серия 18, Социология и политология. — 2018. — Т. 24. — № 1. — С. 52–70.

143. Долгинов, С. Д. Технологии применения видео-конференц-связи на предварительном следствии: проблемы сегодняшнего дня / С. Д. Долгинов // Уголовное право и процесс. — 2023. — С. 470–485.

144. Дяблова, Ю. Л. Некоторые аспекты соотношения раскрытия и расследования преступлений / Ю. Л. Дяблова // Известия Тульского госуниверситета. — 2009. — № 1. — С. 358–363.

145. Ельчанинова, Н. Б. Правовое регулирование споров о доменных именах в сети Интернет / Н. Б. Ельчанинова // Известия ЮФУ. Технические науки. — 2006. — № 10. — С. 206–211.

146. Жарова, А. К. О соотношении персональных данных с IP адресом. Российский и зарубежный опыт / А. К. Жаркова // Вестник УРФО. Безопасность в информационной сфере. — 2016. — № 1. — С. 60–65.

147. Желтобрюхов, С. П. О необходимости предоставления органу предварительного расследования возможности применения видео-конференц-связи на стадии досудебного производства / С. П. Желтобрюхов // Российская юстиция. — 2016. — № 1. — С. 62–64.

148. Зайцев, О. А. Особенности уголовно-процессуального доказывания в условиях цифровизации / О. А. Зайцев // Журнал российского права. — 2024. — № 8. — С. 93–112.

149. Звягин, В. А. Доменное имя — новое средство индивидуализации / В. А. Звягин // Закон и право. — 2010. — № 9. — С. 89–92.

150. Земцова, С. И. Алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов / С. И. Земцова // Современное право. — 2024. — № 3. — С. 45–52.

151. Исаева, К. А. Фальсификация доказательств с использованием дипфейк-технологий / К. А. Исаева, Т. Т. Калиев // Аграрное и земельное право. — 2024. — № 12 (240). — С. 460–462.

152. Ишин, А. М. Современные проблемы использования сети Интернет в расследовании преступлений / А. М. Ишин // Вестник Балтийского федерального университета им. И. Канта. Серия «Гуманитарные и общественные науки». — 2013. — № 9. — С. 116–123.

153. Ищенко, П. П. Следственные действия в условиях цифровизации уголовного судопроизводства / П. П. Ищенко // Сибирские уголовно-процессуальные и криминалистические чтения. — 2022. — № 1. — С. 30–42.

154. Каминский, А. М. Использование электронных криминалистически неупорядоченных банков данных в раскрытии преступлений / А. М. Каминский, Д. А. Овчинникова // Вестник Удмуртского университета. — 2020. — Т. 30. — Вып. 1. — С. 91–98.

155. Качалова, О. В. Уголовно-процессуальные проблемы информатизации современного уголовного судопроизводства / О. В. Качалова // Российское правосудие. — 2019. — № 2. — С. 93–100.

156. Ким, В. Д. Следственная ситуация как поисково-познавательная система в криминалистике / В. Д. Ким // Алтайский юридический вестник. — 2016. — № 3 (15). — С. 125–129.

157. Каримов, В. Х. Актуальные вопросы выявления и расследования преступлений, совершаемых с использованием средств шифрования данных в сети Интернет / В. Х. Каримов // Уголовно-процессуальные и криминалистические

чтения на Алтае : сб. науч. ст. / отв. ред. С. И. Давыдов, В. В. Поляков. Вып. XIV. — Барнаул : Изд-во Алт. ун-та, 2017. — С. 40–47.

158. Климова, Я. А. Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия / Я. А. Климова // Актуальные проблемы российского права. — 2025. — Т. 20. — № 10 (179). — С. 133–143.

159. Койсин, А. А. Правовые основы применения технико-криминалистических средств на предварительном следствии и в суде / А. А. Койсин // Сибирский юридический вестник. — 2007. — № 4.

160. Колиев, В. В. Тактика и методика расследования преступлений, совершаемых с помощью сети «Интернет» / В. В. Колиев // Право и государство: теория и практика. — 2021. — № 4 (196). — С. 280–282.

161. Корма, В. Д. К вопросу о структуре и особенностях криминалистической теории следственного познания / В. Д. Корма, В. А. Образцов // Современные проблемы отечественной криминалистики и перспективы ее развития : сборник научных статей. — Краснодар : Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. — С. 60–66.

162. Корноухов, В. Е. О системах тактических задач и операций при расследовании убийств и их специфике на начальном этапе расследования / В. Е. Корноухов // Проблемы оптимизации первоначального этапа расследования преступлений : межвуз. сб. науч. тр. / отв. ред. И. Ф. Герасимов, Л. Я. Драпкин. — Свердловск : Свердл. юрид. институт, 1988. — С. 85–90.

163. Красненко, Ю. В. Поисково-познавательная деятельность на первоначальном этапе расследования / Ю. В. Красненко // Вестник БелЮИ МВД России. — 2019. — № 3. — С. 52–57.

164. Кувычков, С. И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект / С. И. Кувычков // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2015. — № 2. — С. 76–81.

165. Кустов, А. М. Криминалистическая концепция механизма преступления / А. М. Кустов // Вестник МФЮА. — 2016. — № 2. — С. 164–167.

166. Лавдаренко, Л. И. Раскрытие преступления как одна из задач органов предварительного расследования / Л. И. Лавдаренко // Сибирский юридический вестник. — 2013. — № 1 (60). — С. 98–102.

167. Ладушкин, С. И. Ресурс как проблема логики / С. И. Ладушкин // Проблемы современной науки и образования. — 2015. — № 1 (31).

168. Левгеева, Т. Б. Криминалистический анализ личности преступника, совершившего преступление с использованием интернет-технологий / Т. Б. Левгеева // Исследования молодых ученых : материалы XXX Междунар. науч. конф., г. Казань, янв. 2022 г. — Казань : Молодой ученый, 2022. — С. 33–36.

169. Литвинова, М. А. Особенности субъективной регуляции деятельности следователя в зависимости от ее сложности / М. А. Литвинова // Вестник Самарского юридического института. — 2020. — № 3. — С. 117–126.

170. Ляховская, А. А. Ник: специфика, графическое оформление и функции / А. А. Ляховская // Вестник Полоцкого государственного университета. Серия А, Гуманитарные науки. 2010. — № 7. — С. 154–161.

171. Мазунин, Я. М. Организационные особенности производства допроса с использованием видеоконференц-связи / Я. М. Мазунин, К. С. Сидорова // Технологии XXI века в юриспруденции : материалы Всероссийской научно-практической конференции (Екатеринбург, 24 мая 2019 г.). — Екатеринбург : Уральский государственный юридический университет, 2019. — С. 98–102.

172. Мазунин, Я. М. Особенности фиксации допроса, проводимого с использованием видеоконференцсвязи [Электронный ресурс] / Я. М. Мазунин, К. С. Белова // Технологии XXI века в юриспруденции : материалы Четвертой международной научно-практической конференции (Екатеринбург, 20 мая 2022 г.) / отв. ред. Д. В. Бахтеев. — Екатеринбург : Уральский государственный юридический университет имени В.Ф. Яковлева, 2022. — С. 27–30. 1 CD-ROM.

173. Мазунин, Я. М. Следственные ситуации и алгоритм их разрешения при расследовании мошенничеств, совершаемых дистанционным способом

в современных условиях / Я. М. Мазунин, К. С. Сидорова // Технологии XXI века в юриспруденции : материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 г.) / под ред. Д. В. Бахтеева. — Екатеринбург : Уральский государственный юридический университет, 2020. — С. 465–470.

174. Мазунин, Я. М. Розыскная деятельность следователя в информационно-телекоммуникационной сети «Интернет» / Я. М. Мазунин, К. С. Сидорова // Актуальные проблемы правоприменительной деятельности органов внутренних дел : сборник научных трудов. Т. 4. — Омск : Омская академия Министерства внутренних дел Российской Федерации, 2019. — С. 186–212.

175. Малахов, А. С. Обнаружение сведений о криминальных событиях с использованием интернет-поисковых систем при раскрытии и расследовании преступлений [Электронный ресурс] / А. С. Малахов, К. С. Сидорова // 100 лет уголовному розыску России: история, современность, перспективы : материалы всероссийской научно-практической конференции, Санкт-Петербург, 8 ноября 2018 г. / сост. М. Л. Родичев. — СПб. : Санкт-Петербургский университет МВД России, 2018. — С. 102–106. — 1 электрон. опт. диск.

176. Маркелов, А. Г. Особенности проведения отдельных следственных действий с использованием инновационных технологий по уголовным делам в сфере экономики / А. Г. Маркелов, М. А. Нефедов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2015. — № 1. — С. 136–139.

177. Марковичева, Е. В. Перспективы развития электронного судопроизводства в Российской Федерации / Е. В. Марковичева // Российское правосудие. — 2017. — № 3 (131). — С. 88–95.

178. Масленникова, Л. Н. Концептуальный подход к построению уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий / Л. Н. Масленникова // Вестник Университета имени О.Е. Кутафина. — 2020. — № 10 (74).

179. Медведева, Т. М. Если у налогоплательщика и его контрагента один IP-адрес / Т. М. Медведева // Актуальные вопросы бухгалтерского учета и налогообложения. — 2017. — № 10. — С. 63–69.

180. Меретуков, Г. М. Еще раз об объекте и предмете криминалистики / Г. М. Меретуков // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — 2014. — № 96. — С. 633–652.

181. Меретуков, Г. М. Особенности использования искусственного интеллекта в криминалистической деятельности: некоторые актуальные вопросы / Г. М. Меретуков, А. С. Усенко // Вестник Томского государственного университета. Право. — 2025. — № 57. — С. 44–58.

182. Михайлов, М. А. Будущее следственных действий в эпоху информационных технологий: эволюция или революция / М. А. Михайлов // Уголовное производство: процессуальная теория и криминалистическая практика : материалы VI Междунар. науч.-практ. конф. — Симферополь : Ариал, 2018. — С. 72–74.

183. Михайлов, А. И. Процессуальная сущность раскрытия преступления / А. И. Михайлов, Л. А. Сергеев // Советское государство и право. — 1971. — № 4. — С. 110–115.

184. Мысливцева, Т. Ю. Тактические рекомендации при допросах по уголовным делам, связанным с незаконным оборотом наркотических средств, совершенным с использованием сети Интернет / Т. Ю. Мысливцева // Российский следователь. — 2023. — № 2. — С. 2–6.

185. Низамов, В. Ю. К вопросу о понятии «раскрытие преступления» в криминалистике и уголовном процессе / В. Ю. Низамов // Ленинградский юридический журнал. — 2016. — № 1 (43). — С. 170–179.

186. Нестеров, В. С. Использование цифровых технологий при фальсификации доказательств в досудебном производстве по уголовным делам / В. С. Нестеров // Гуманитарные, социально-экономические и общественные науки. — 2025. — № 8. — С. 132–136.

187. Олиндер, Н. В. Проблемные вопросы поиска и восприятия информации о человеке в сети интернет и ее использование при расследовании преступлений / Н. В. Олиндер, Е. А. Гамбарова // Юридический вестник Самарского университета. — 2016. — Т. 2. — № 4. — С. 55–59.

188. Павлов, А. В. Получение и использование сведений с сайтов социальных интернет-сетей для установления местонахождения подозреваемого (обвиняемого), находящегося в розыске / А. В. Павлов, К. С. Сидорова // Законодательство и практика. — 2017. — № 1 (38). — С. 14–16.

189. Павлов, С. П. Производство следственных действий с применением видео-конференц-связи / С. П. Павлов // Молодой ученый. — 2023. — № 12 (459). — С. 103–104.

190. Пашутина, О. С. Очная ставка: проблемные аспекты уголовно-процессуального регулирования / О. С. Пашутина, Д. В. Алымов // Российский следователь. — 2020. — № 6. — С. 13–16.

191. Першин, А. Н. Использование ресурсов информационно-телекоммуникационной сети интернет в розыскной деятельности следователя / А. Н. Першин, К. С. Сидорова // Библиотека криминалиста. — 2017. — № 4. — С. 320–328.

192. Першин, А. Н. Криминалистические основы установления пользователя информационно-телекоммуникационной сети интернет / А. Н. Першин, К. С. Сидорова // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 3 (55). — С. 82–94.

193. Першин, А. Н. Направления использования информационно-телекоммуникационной сети «Интернет» в расследовании преступлений / А. Н. Першин, К. С. Сидорова // Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы : сборник научных статей Международной научно-практической конференции, Москва, 25–26 мая 2017 г. / под ред. И. П. Можаевой. — М. : Академия управления Министерства внутренних дел РФ, 2017. — С. 458–462.

194. Поликарпов, Е. С. О некоторых аспектах идентификации пользователя сети интернет / Е. С. Поликарпов, С. Л. Анисимов // Охрана, безопасность, связь. — 2017. — № 1-2. — С. 105–112.

195. Поддубняк, А. А. Допрос свидетеля посредством видео-конференц-связи на стадии предварительного расследования как новелла российского законодательства / А. А. Поддубняк, И. С. Евдокимова // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. — 2018. — № 3. — Т. 4. — С. 159–165.

196. Поляков, В. В. Особенности производства осмотра по компьютерным преступлениям / В. В. Поляков // Российский следователь. — 2017. — № 21. — С. 14–17.

197. Поляков, В. В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы / В. В. Поляков, А. С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае. Вып. XIV. — Барнаул : Изд-во Алт. ун-та, 2017. — С. 96–101.

198. Поляков, В. В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике / В. В. Поляков, А. В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. — 2013. — № 11-1. — С. 123–145.

199. Попов, А. М. Особенности производства осмотра по преступлениям в сфере компьютерной информации как элемент доказывания / А. М. Попов, А. И. Дубовицкий // Право: история и современность. — 2020. — № 1 (10). — С. 109–115.

200. Потапов, А. В. Возможности применения сети Интернет в расследовании преступлений: тактические и правовые аспекты / А. В. Потапов // NovaInfo.Ru. — 2017. — № 58. — Т. 4. — С. 363–367.

201. Пропастин, С. В. Осмотр, обыск или судебная экспертиза: проблема выбора при расследовании преступлений, совершаемых с использованием

интернет-технологий / С. В. Пропастин // Научный вестник Омской академии МВД России. — 2015. — № 2. — С. 20–23.

202. Протасевич, А. А. Методология криминалистического учения о человеке и человеческой деятельности / А. А. Протасевич, Е. И. Фойгель // Всероссийский криминологический журнал. — 2017. — Т. 11. — № 3. — С. 590–602.

203. Пшегорская, Ю. В. Типология молодежных сетевых имен, функционирующих в современном русскоязычном сегменте интернета / Ю. В. Пшегорская // Филологические науки. Вопросы теории и практики. — 2014. — № 1-1. — С. 150–154.

204. Рамалданов, Х. Х. Видеопротоколирование как основа цифровизации уголовного судопроизводства / Х. Х. Рамалданов // Юристъ-Правоведъ. — 2022. — № 4 (103). — С. 86–92.

205. Родивилин, И. П. Использование компьютерной информации при раскрытии и расследовании преступлений, совершенных с использованием сети интернет / И. П. Родивилин // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. — Иркутск : Восточно-Сибирский институт МВД России, 2015. — С. 173–178.

206. Родивилина, В. А. Некоторые вопросы применения видео-конференц-связи в досудебном производстве / В. А. Родивилина // Вестник Иркутского государственного технического университета. — 2015. — № 2 (97). — С. 278–280.

207. Романова, Л. И. Личность интернет-преступника / Л. И. Романова // Азиатско-Тихоокеанский регион: экономика, политика и право. — 2018. — № 3. — С. 155–169.

208. Романова, Л. И. Преступный мир Darknet / Л. И. Романова, Р. И. Дремлюга // Юридическая наука и практика. — 2018. — Т. 14. — № 1. — С. 52–60.

209. Россинская, Е. Р. Тренды развития криминалистики в условиях цифровой трансформации современной преступности / Е. Р. Россинская // Союз криминалистов и криминологов. — 2025. — № 1. — С. 162–173.

210. Руденко, А. В. Проблема определения понятия, предмета и объекта криминалистики / А. В. Руденко // Теория и практика общественного развития. 2014. — № 6. — С. 171–173.

211. Рудневский, А. В. Определение местоположения по базовым станциям в сетях GSM / А. В. Рудневский // Беспроводные технологии. — 2010. — № 20. — Т. 3. — С. 16–18.

212. Румянцева, И. В. Роль криминалистической диагностики механизма преступления в установлении обстоятельств, подлежащих доказыванию / И. В. Румянцева // Преступность в Западной Сибири: актуальные проблемы профилактики и расследования преступлений : сб. науч. статей. — Тюмень : Тюменский государственный университет, 2013. — С. 430–434.

213. Русскевич, Е. А. О совокупности преступлений в сфере компьютерной информации с другими преступлениями / Е. А. Русскевич // Уголовное право. — 2025. — № 4. — С. 76–84.

214. Рябчиков, С. А. Видеопротоколирование как средство уголовно-процессуального доказывания / С. А. Рябчиков // Вестник ЮУрГУ. Серия «Право». — 2024. — Т. 24. — № 2. — С. 56–62. — DOI: 10.14529/law240209.

215. Рянская, Э. М. Сетевое имя (никнейм) как языковой знак / Э. М. Рянская, А. С. Балкунова // Вестник Нижневартовского государственного гуманитарного университета. — 2011. — № 4. — С. 72–76.

216. Сайгачева, И. А. Методика расследования преступлений экстремистской направленности, совершенных в компьютерных сетях / И. А. Сайгачева // Контентус. — 2025. — № 12 (161). — С. 14–22.

217. Сафронов, Д. М. Уголовно-процессуальные и криминалистические аспекты получения информации о пользователях сети Интернет при производстве следственных действий / Д. М. Сафронов, К. С. Сидорова // Российская юстиция. — 2021. — № 1. — С. 30–33.

218. Сидорова К. С. Криминалистически значимые сведения, получаемые из ресурсов информационно-телекоммуникационной сети «интернет» в ходе расследования преступлений / К. С. Сидорова // Современные тенденции развития

юридической науки : материалы международной научно-теоретической конференции молодых ученых, посвященной Дню казахстанской науки / под общ. ред. канд. юрид. наук, доцента А. Дарменова. — Караганда : Карагандинская академия МВД Республики Казахстан имени Б. Бейсенова, 2022. — С. 70–72.

219. Сидорова, К. С. IP-адрес как один из идентификаторов личности в расследовании преступлений / К. С. Сидорова // Психопедагогика в правоохранительных органах. — 2018. — № 3 (74). — С. 84–87.

220. Сидорова, К. С. Направления поисковых действий следователя в информационно-телекоммуникационной сети «Интернет» при расследовании преступлений / К. С. Сидорова // Актуальные проблемы расследования преступлений : материалы Всероссийской научной конференции памяти И. Ф. Герасимова (Екатеринбург, 31 января 2020 года) / под ред. Д. В. Бахтеева. — Екатеринбург : Уральский государственный юридический университет, 2020. — С. 135–143.

221. Сидорова, К. С. Особенности производства допроса с использованием видеоконференцсвязи / К. С. Сидорова // Криминалистика: актуальные вопросы теории и практики : материалы междунар. науч.-практ. конф. — Ростов-н/Д. : Ростовский юридический институт МВД России, 2019. — С. 193–199.

222. Сидорова, К. С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел / К. С. Сидорова // Вестник Сибирского института бизнеса и информационных технологий. — 2018. — № 2 (26). — С. 88–92.

223. Сидорова, К. С. Способы фиксации информации, полученной с использованием ресурсов сети Интернет / К. С. Сидорова // Преемственность и новации в юридической науке : Материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей, Омск, 21 мая 2019 г. — Омск : Омская академия Министерства внутренних дел РФ, 2019. — С. 95–97.

224. Сидорова, К. С. Тактические особенности осмотра интернет-страницы в ходе расследования преступлений / К. С. Сидорова // Проблемы криминалистической науки, следственной и экспертной практики : сборник

научных трудов / пред. редколлегии Я. М. Мазунин. Вып. 11. — Омск : Омская академия Министерства внутренних дел РФ, 2021. — С. 53–56.

225. Сидорова, К. С. Алгоритм действий следователя при расследовании мошенничеств, совершаемых дистанционным способом / К. С. Сидорова // Закон и право. — 2020. — № 12. — С. 230–233.

226. Сидорова, К. С. Обстоятельства, выясняемые у подозреваемого (обвиняемого) в ходе допроса об использовании им коммуникационных технологий через сеть интернет / К. С. Сидорова // Преемственность и новации в юридической науке : материалы Всероссийской научной конференции адъюнктов, аспирантов и соискателей (Омск, 28 марта 2017 г.) / отв. за вып. канд. юрид. наук И. В. Сидорова. — Вып. 13. — Омск : Омская академия МВД России, 2017. — С. 86–88.

227. Сидорова, К. С. Особенности получения криминалистически значимой информации из сети Интернет / К. С. Сидорова // Расследование уголовных правонарушений в сети Интернет: проблемы и пути решения : сб. материалов круглых столов. — Косшы : Академия правоохранительных органов при Генеральной прокуратуре РК, 2021. — 192 с.

228. Сидорова, К. С. Следственные ситуации и алгоритм их разрешения при установлении пользователя информационно-телекоммуникационной сети «Интернет» / К. С. Сидорова // Вклад Л. Я. Драпкина в криминалистическую науку : материалы Всероссийского научно-практического круглого стола (Екатеринбург, 1 ноября 2019 года). — Екатеринбург : Уральский государственный юридический университет, 2019. — С. 258–266.

229. Скворцов, Р. И. Уголовно-процессуальные и тактические основы применения технических средств при производстве следственных действий / Р. И. Скворцов // Общество и право. — 2013. — № 4 (46). — С. 188–191.

230. Скобелин, С. Ю. Использование специальных знаний при работе с электронными следами / С. Ю. Скобелин // Российский следователь. — 2014. — № 20. — С. 31–33.

231. Скорик, Г. В. Человек в информационном обществе: проблема идентификации (поиска идентичности) / Г. В. Скорик // Вестник Томского государственного университета. — 2007. — № 302. — С. 50–58.

232. Смагин, П. Г. Использование информационных сервисов сети Интернет при расследовании преступлений / П. Г. Смагин, С. В. Лемайкина, А. Г. Карпика // Актуальные проблемы теории и практики уголовного процесса : сб. материалов Междунар. науч.-практ. конф. — Ростов н/Д. : Ростовский юридический институт МВД России, 2018. — С. 35–41.

233. Смушкин, А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / А. Б. Смушкин // Актуальные проблемы российского права. — 2022. — Т. 17. — № 3. — С. 102–111. — DOI: 10.17803/1994-1471.2022.136.3.102-111.

234. Соколова, Е. А. Конкуренция информации в законодательстве РФ о товарных знаках и правовых нормах РФ о доменных именах / Е. А. Соколова // Законы России: опыт, анализ, практика. — 2010. — № 4. — С. 57–61.

235. Соколова, Т. П. Нейминговая экспертиза: генезис, проблемы, перспективы / Т. П. Соколова // Вестник Университета имени О.Е. Кутафина. — 2014. — № 3. — С. 140–152.

236. Стельмах, В. Ю. Порядок производства следственных действий по видео-конференц-связи / В. Ю. Стельмах // Российский судья. — 2022. — № 10. — С. 25–29.

237. Сумин, С. А. Применение систем видео-конференц-связи при допросе защищаемых территориально удаленных лиц, участвующих в уголовном судопроизводстве на стадиях предварительного и судебного следствия: проблемы реализации и повышение эффективности / С. А. Сумин // Вестник Воронежского института МВД России. — 2011. — № 3. — С. 68–75.

238. Тагиров, З. И. Цифровая оперативная обстановка, цифровое имя человека и сетевая (цифровая) правоохранительная деятельность в отечественной модели цифровой экономики / З. И. Тагиров // Вопросы безопасности. — 2018. — № 4. — С. 28–51.

239. Тишутина, И. В. Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий: актуальные вопросы правового обеспечения / И. В. Тишутина // Вестник Московского университета МВД России. — 2021. — № 4. — С. 280–282.

240. Трофимов, Е. И. Электронная подпись как средство защиты электронных документов от подделки / Е. И. Трофимов // Педагогическое образование на Алтае. — 2014. — № 2. — С. 446–447.

241. Туркулец, В. А. Типология личности преступника, совершающего преступления против несовершеннолетнего с использованием сети Интернет / В. А. Туркулец, И. А. Туркулец, С. Е. Туркулец // Право и практика. — 2025. — № 1. — С. 130–138.

242. Узденов, Р. М. Новые границы киберпреступности / Р. М. Узденов // Всероссийский криминологический журнал. — 2016. — Т. 10. — № 4. — С. 645–655.

243. Фокин, А. Д. Принципы и тактика проведения следственного осмотра интернет-ресурса при расследовании дистанционного мошенничества в сфере недвижимости / А. Д. Фокин // Российский следователь. — 2025. — № 3. — С. 2–7.

244. Фомина, И. А. Использование искусственного интеллекта в криминалистическом анализе: отдельные проблемы теории и практики / И. А. Фомина // Сибирский юридический вестник. — 2026. — № 1 (112). — С. 103–109

245. Черданцев, А. Ю. Практические проблемы получения, анализа и последующей правильной интерпретации полученной цифровой криминалистически значимой информации / А. Ю. Черданцев // Эксперт-криминалист. — 2022. — № 4. — С. 26–29.

246. Черкасов, В. С. Проблема разграничения следственных действий: осмотр и обыск при получении компьютерной информации / В. С. Черкасов // Правопорядок: история, теория, практика. — 2018. — № 1 (16). — С. 99–104.

247. Чупилкин, Ю. Б. Содержание категорий «раскрытие», «расследование» и «раскрываемость» преступлений в российском законодательстве / Ю. Б. Чупилкин // Российская юстиция. — 2019. — № 4. — С. 32–35.

248. Шаповалова, Г. М. Электронные документы в уголовном судопроизводстве и криминалистике / Г. М. Шаповалова // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. — 2015. — № 12-4. — С. 199–202.

249. Шаров, В. И. Оперативно-розыскные мероприятия в сети Интернет / В. И. Шаров // Общество и право. — 2018. — № 2 (64). — С. 82–87.

250. Шевчук, В. М. Тактические задачи и формирование тактических операций в досудебном производстве / В. М. Шевчук // Электронный журнал «Вестник МГОУ». — 2013. — № 1.

251. Шевчук, В. М. Роль факторов-детерминантов формирования тактических операций при расследовании преступлений / В. М. Шевчук // Психопедагогика в правоохранительных органах. — 2013. — № 2 (53). — С. 30–38.

252. Шестакова, С. Д. О новых подходах к процессуальному значению материалов аудио- и видеозаписи, применяемых при производстве следственных действий, в условиях цифровизации / С. Д. Шестакова, С. Л. Виноградова // Уголовное судопроизводство России: проблемы и перспективы развития : материалы всерос. науч.-практ. конф. — СПб., 2020. — С. 393–396.

253. Шурухнов, Н. Г. Правовые и информационно-технические процедуры производства допроса посредством систем видео-конференц-связи (анализ отдельных положений ст. 189.1 УПК РФ) / Н. Г. Шурухнов // Российский следователь. — 2022. — № 7. — С. 26–30.

254. Якунин, С. Ю. Тактические задачи при расследовании преступлений: понятие и виды / С. Ю. Якунин // Ученые записки Казанского государственного университета. Гуманитарные науки. — 2010. — Т. 152. — Кн. 4. — С. 204–212.

255. Зуев, С. В. Цифровое видеопротоколирование следственных действий: возможности и перспективы / С. В. Зуев // Ученые записки : сб. науч. тр., Оренбург, 14–15 нояб. 2019 г. — Оренбург : РПК Полиарт, 2020. — С. 7–10.

256. Эксархопуло, А. П. О предмете криминалистики и его определении / А. П. Эксархопуло // Вестник криминалистики. — 2003. — Вып. 4 (8). — С. 19–28.

257. Якунина, М. Л. Особенность интернет-дискурса: никнейм / М. Л. Якунина // Филологические науки. Вопросы теории и практики. — 2013. — № 3-2. — С. 218–221.

258. Якушин, С. Ю. Тактические задачи при расследовании преступлений: понятие и виды / С. Ю. Якушин // Ученые записки Казанского государственного университета. Гуманитарные науки. — 2010. — Т. 152. — Кн. 4. — С. 204–212.

## 5. Диссертации и авторефераты диссертаций

259. Асмус, Н. Г. Лингвистические особенности виртуального коммуникативного пространства : дис. …канд. филол. наук : 10.02.19 / Асмус Нина Геннадьевна. — Челябинск, 2005. — 266 с.

260. Балашова, А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : автореф. дис. … канд. юрид. наук : 12.00.09 / Балашова Анна Александровна. — М., 2020. — 24 с.

261. Балкунова, А. С. Роль сетевого имени (никнейма) во взаимодействии субъектов виртуальной коммуникации : дис. … канд. филол. наук : 10.02.19 / Балкунова Александра Сергеевна. — М., 2012. — 261 с.

262. Бахтеев, Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : дис. … д-ра юрид. наук : 5.1.4 / Бахтеев Дмитрий Валерьевич. — Екатеринбург, 2022. — 504 с.

263. Демидов, Н. Н. Изучение личности преступника в процессе расследования : дис. канд. юрид. наук : 12.00.09 / Демидов Николай Николаевич. — Волгоград, 2003. — 189 с.

264. Ефремова, О. М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве

следственных действий : автореф. дис. … канд. юрид. наук : 12.00.09 / Ефремова Ольга Михайловна. — Орел, 2021. — 26 с.

265. Завьялов, В. А. Формирование и реализация тактических операций : дис. … канд. юрид. наук : 12.00.12 / Завьялов Владимир Александрович. — Краснодар, 2021. — 195 с.

266. Зазулин, А. И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : дис. … канд. юрид. наук : 12.00.09 / Зазулин Анатолий Игоревич. — Екатеринбург, 2018. — 280 с.

267. 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.

268. Лубин, А. Ф. Методология криминалистического исследования механизма преступной деятельности : дис. ... д-ра юрид. наук : 12.00.09 / Лубин Александр Федорович. — Н. Новгород, 1997. 337 с.

269. Лузгин, И. М. Расследование как процесс познания : дис. ... д-ра юрид. наук / Лузгин Игорь Михайлович. — М., 1969. — 328 с.

270. Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук : 12.00.09 / Мещеряков Владимир Алексеевич. — Воронеж, 2001. — 386 с.

271. Оконенко, Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе : дис. … канд. юрид. наук : 12.00.09 / Оконенко Роман Иванович. — М., 2016. — 156 с.

272. Поляков, В. В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. … канд. юрид. наук : 12.00.09 / Поляков Виталий Викторович. — Омск, 2008. — 247 с.

273. Себякин, А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации : автореф. дис. … канд. юрид. наук : 12.00.12 / Себякин Алексей Геннадьевич. — М., 2021. — 26 с.

274. Степаненко, Д. А. Проблемы теории и практики криминалистической идентификации : дис. …д-ра юрид. наук : 12.00.09 / Степаненко Диана Аркадьевна. — Иркутск, 2006. — 337 с.

275. Судницын, А. Б. Задачи предварительного расследования : автореф. дис. … канд. юрид. наук : 12.00.09 / Судницын Алексей Борисович. — Омск, 2009. — 24 с.

276. Фокин, А. Д. Теоретико-прикладные основы методики расследования мошенничества в сфере оборота жилых помещений, совершаемого с использованием информационно-телекоммуникационных технологий : дис. … канд. юрид. наук : 5.1.4 / Фокин Андрей Денисович. — М., 2025. — 225 с.

277. Черкасов, В. С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса : дис. … канд. юрид. наук : 12.00.09 / Черкасов Виктор Сергеевич. — Хабаровск, 2022. — 240 с.

## 6. Электронные ресурсы

278. 15 лучших программ для распознавания речи 2025 года [Электронный ресурс] // Режим доступа: https://transkriptor.com/ru.

279. Батищев, П. С. Основы Интернет [Электронный ресурс] / П. С. Батищев // Режим доступа: https://psbatishev.narod.ru/internet/12.htm.

280. Безопасность пользователей в сети Интернет [Электронный ресурс] // Режим доступа: https://safe-surf.ru/users-of/article/228/.

281. В России вступили в силу новые правила идентификации в мессенджерах [Электронный ресурс] // Режим доступа: https://ria.ru/amp/20190505/1553265286.html.

282. Веб-конференция в Верховном Суде Российской Федерации [Электронный ресурс] // Режим доступа: https://vsrf.ru/press_center/news/28867/.

283. ВС включил мессенджеры в инструменты совершения киберпреступлений [Электронный ресурс] // Режим доступа: https://rapsi-pravo.ru/judicial_analyst/20230914/309217921.html.

284. Глоссарий интернет-маркетинга [Электронный ресурс] // Режим доступа: https://www.glossary-internet.ru.

285. Голованов, В. Gopher, конкурент WWW из 90-х, который пока не стоит списывать со счетов [Электронный ресурс] / В. Голованов // Режим доступа: https://habr.com/ru/articles/581692/.

286. Ефремова, Т. Ф. Новый словарь русского языка. Толково-словообразовательный [Электронный ресурс] / Т. Ф. Ефремова. — М. : Русский язык, 2000. — Режим доступа: https://www.efremova.info/word/raskrytie.html.

287. Зверев, Д. Протокол FTP: что это такое и как с ним работать [Электронный ресурс] / Д. Зверев // Режим доступа: https://skillbox.ru/media/code/protokol-ftp-chto-eto-takoe-i-kak-s-nim-rabotat/.

288. Земцова, С. И. Алгоритм осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием интернет-магазинов [Электронный ресурс] / С. И. Земцова, П. В. Галушин // Режим доступа: https://www.sovremennoepravo.ru/.

289. Конин, А. В. Раскрытие преступления: субъекты и алгоритм [Электронный ресурс] / А. В. Конин, С. А. Ялышев // Режим доступа: https://procuror.spb.ru/k213714.html.

290. Краткая характеристика ресурсов Интернета [Электронный ресурс] // Режим доступа: https://opengl.org.ru/informatsionnye-sistemy-i-tekhnologii-v-zkonomike/kratkaya-kharakteristika-resursov-interneta.html.

291. Кузьмин, Д. Как превратить голос в текст: тестируем 6 сервисов для расшифровки / Д. Кузьмин [Электронный ресурс] // Режим доступа: https://journal.tinkoff.ru/list/voice-txt/.

292. Лингвистическая экспертиза [Электронный ресурс] // Режим доступа: http://www.sudexpert.ru/possib/lingv.php.

293. Логин [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Логин.

294. Лопатина, В. Цифровой профиль гражданина: что это и чем полезен организациям [Электронный ресурс] / В. Лопатина // Режим доступа: https://www.softlab.ru/blog/citizen-digital-profile.

295. МВД России публикует статистическую информацию о состоянии преступности в Российской Федерации за январь — ноябрь 2025 года [Электронный ресурс] // Режим доступа: https://mvdmedia.ru/news/official/informatsiya-o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-za-yanvar-noyabr-2025-goda/.

296. Мобильный криминалист [Электронный ресурс] // Режим доступа:: https://www.tadviser.ru/index.php.

297. Основы информационно-библиографической культуры : электронное учеб.-метод. пособие НИЯУ МИФИ [Электронный ресурс] // Режим доступа: http://library.mephi.ru/icb2/glav5_new.html.

298. Перевод аудио в текст: ТОП 5 программ для распознавания речи [Электронный ресурс] // Режим доступа: https://eks-libris.ru/blog/perevod-audio-v-tekst-top-5-programm-dlya-raspoznavaniya-rechi/.

299. Сегодня интернет переходит на новый протокол IPv6 [Электронный ресурс] // Режим доступа: https://ain.ua/2012/06/06/segodnya-internet-perexodit-na-novyj-protokol-ipv6.

300. Сергеевичева, Н. В. Основы самостоятельной и исследовательской работы (КМТ) [Электронный ресурс] / Н. В. Сергеевичева // Режим доступа: https://a-pet.ru/moodle/mod/page/view.php?id=43253.

301. Словарь русского языка : в 4 т. [Электронный ресурс] / РАН, Ин-т лингвистич. исследований ; под ред. А. П. Евгеньевой. — 4-е изд., стер. — М. : Рус. яз. ; Полиграфресурсы, 1999. — Фундаментальная электронная библиотека. — Режим доступа: https://kartaslov.ru.

302. Статистика пользователей интернета в мире и в России [Электронный ресурс] // Режим доступа: https://up-advert.ru/blog/digital-2025/.

303. Суд рассмотрит дело о легализации средств через сайты знакомств и фишинг [Электронный ресурс] // Режим доступа: https://rapsinews.ru/judicial_news/20250129/310587639.html.

304. Методические рекомендации Минцифры России от 02.04.2021 «Сценарии использования инфраструктуры Цифрового профиля. Версия 1.2» [Электронный ресурс] // Режим доступа: https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv12.pdf.

305. Толковый словарь Ожегова [Электронный ресурс] // Режим доступа: https://slovarozhegova.ru/.

306. Форум «ПравоТех» [Электронный ресурс] // Режим доступа: https://pravo.tech.

307. Решение председателя Гостехкомиссии России от 30.03.1992 [Электронный ресурс] // ФСТЭК России : официальный сайт. — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3.

308. Что такое WHOIS [Электронный ресурс] // Режим доступа: https://handyhost.ru/help/term/chto-takoe-whois.html.

309. Шевчук, В. М. Тактические задачи и формирование тактических операций в досудебном производстве [Электронный ресурс] / В. М. Шевчук // Режим доступа: https://evestnik-mgou.ru/ru/Articles/Doc/307.

310. AI в законе: суды в России оценивают искусственный интеллект как естественный [Электронный ресурс] // Режим доступа: https://www.fontanka.ru/2025/12/14/76171234/.

311. Google помогает полиции определять устройства вблизи мест преступления, используя данные о местоположении [Электронный ресурс] // Режим доступа: https://habr.com/ru/articles/448562/.

312. Velter Tech Blog [Электронный ресурс] // Режим доступа: https://velter.tech/blog/tpost/in1chgep81-kak-produkti-velter-pomogayut-raskrivat.

# ПРИЛОЖЕНИЯ

*Приложение 1*

## Результаты анкетирования работников подразделений органов следствия и дознания по вопросам использования информационно-телекоммуникационной сети «Интернет» при расследовании преступлений

Эмпирическую базу исследования составили результаты анкетирования и интервьюирования 184 сотрудников органов предварительного расследования. В качестве респондентов выступили следователи и руководители следственных подразделений Следственного комитета РФ, а также следователи и дознаватели органов внутренних дел из 10 субъектов Российской Федерации: Республики Башкортостан, Алтайского, Пермского, Приморского краев, Ленинградской, Московской, Омской, Орловской, Свердловской областей, Ямало-Ненецкого автономного округа.

| № п/п | Вопрос | Ответ |
|---|---|---|
| 1 | **Укажите Вашу должность.** | |
| | Руководитель следственного органа | 13 % |
| | Следователь | 62 % |
| | Дознаватель | 25 % |
| 2 | **Укажите Вашу специализацию.** | |
| | Расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий | 58 % |
| | Расследование преступлений различных категорий | 42 % |
| 3 | **Укажите Ваш стаж работы.** | |
| | До года | 7 % |
| | От года до трех лет | 16 % |
| | От 3 до 5 лет | 36 % |
| | От 5 до 10 лет | 32 % |
| | От 10 до 15 лет | 5 % |
| | Свыше 15 лет | 4 % |
| 4 | **Как часто перечисленные интернет-ресурсы Вы используете в деятельности по расследованию преступлений?** | |

| | | |
|---|---|---|
| | Электронная почта (e-mail) | частота использования: 84 % |
| | Информационная сеть WWW | частота использования: 23 % |
| | Электронные доски объявлений BBS | 0 % |
| | Системы телеконференций, например Usenet | 0 % |
| | Система файловых архивов FTP (File Transfer Protocol — «протокол передачи файлов») | 0 % |
| | Информационные системы, например Gopher | 0 % |
| | Информационные ресурсы, например LISTSER V | 0 % |
| | Каталоги X.500 | 0 % |
| | Справочные службы, например WHOIS | частота использования: 38 % |
| | Система TRICKLE | 0 % |
| | Протоколы для удаленного доступа к ресурсам (например, Telnet) | 0 % |
| | Совокупность различных мессенджеров и социальных сетей | частота использования: 96 % |
| | Электронные торговые площадки (агрегаторы товаров и услуг, маркетплейсы). | частота использования: 42 % |
| | Нейросети | частота использования:<br>ChatGPT — 94%;<br>Deep Seek — 83%;<br>GigaChat — 44 %;<br>You.com — 1 % |
| 5 | **Используете ли Вы сеть «Интернет» при расследовании преступлений? Если да, то в каких целях?** | |
| | В целях розыска информации об участнике уголовного судопроизводства на официальных сайтах органов государственной власти, сайтах социальных сетей, в поисковой системе браузера | 67 % |
| | В целях установления местонахождения интересующего лица по IP-адресу, доменному имени, логину/никнейму | 4 % |
| | В целях розыска похищенного имущества на сайтах онлайн-продаж («Авито», МЛСН и др.) | 10 % |
| | В целях установления провайдера и его географического местоположения по IP-адресу (2ip.ru, ripe.net и др.) | 19 % |
| | Иное | |
| 6 | **По Вашему мнению, ответы на запросы от провайдеров, администраторов сайтов необходимо рассматривать в качестве:** | |
| | Доказательства | 77 % |
| | Ориентирующей информации | 23 % |
| 7 | **Считаете ли Вы целесообразным использовать и приобщать в качестве доказательства в рамках уголовного дела ответы на запросы от организаций-провайдеров и администраторов интернет-сайтов?** | |
| | Да, считаю целесообразным их использовать. Необходимо их осматривать и приобщать к материалам уголовного дела в качестве доказательства — иного документа. | 83 % |

| | | |
|---|---|---|
| | Да, считаю целесообразным их использовать, но в качестве ориентирующей информации. | 17 % |
| | Иное | |
| 8 | **Какие сложности у Вас возникают при фиксации информации с интернет-страницы?** | |
| | Недостаток знаний в области специальной компьютерной терминологии | 33 % |
| | Отсутствие формы протокола осмотра интернет-страницы | 49 % |
| | Иное: отсутствие единой методики изъятия электронной информации | 18 % |
| 9 | **При направлении запроса провайдерам, администраторам сайтов в какие сроки Вы получаете ответы?** | |
| | До 10 дней | 4 % |
| | От 10 до 20 дней | 8 % |
| | От 21 до 30 дней | 33 % |
| | Свыше 30 дней | 51 % |
| | Не получаем | 4 % |
| 10 | **В какие сроки чаще всего Вы получаете ответ на международный запрос о правовой помощи (когда запрос направляется в другое государство с целью получения сведений с сервера интернет-ресурса)?** | |
| | до 6 месяцев | 0 % |
| | от 6 до 12 месяцев | 24% |
| | от 12 месяцев и свыше | 36 % |
| | ответ не поступает спустя год и более | 40 % |
| 11 | **Назначали ли Вы лингвистическую экспертизу по доменным именам, никнеймам (логинам)?** | |
| | Назначал лингвистическую экспертизу по доменным именам | 9 % |
| | Назначал лингвистическую экспертизу по никнеймам при наличии переписки пользователей | 26 % |
| | Не назначал | 55 % |
| 12 | **По каким причинам нецелесообразно назначать лингвистические экспертизы по доменным именам, никнеймам (логинам)?** | |
| | Отсутствие специалиста в области лингвистики | 44 % |
| | Нерентабельно | 11 % |
| | Занимает продолжительный промежуток времени | 32 % |
| | Нецелесообразно назначать экспертизу, т.к. эффективнее использовать помощь специалиста | 13 % |
| | Иное | |
| 13 | **Используете ли Вы при производстве следственных действий технологию видео-конференц-связи? Если да, то при производстве каких следственных действий?** | |
| | Допрос потерпевшего, свидетеля | 3 % |
| | Допрос подозреваемого (обвиняемого) | 0 % |
| | Очная ставка | 0 % |
| | Предъявление для опознания | 0 % |

| | | |
|---|---|---|
| | Иное: нет технической возможности для производства следственных действий с использованием видео-конференц-связи;<br>отсутствуют тактика и методика производства следственных действий с использованием видео-конференц-связи | 44%<br><br><br>53 % |
| 14 | **Если бы имелась техническая возможность для производства следственных действий с использованием видео-конференц-связи, то в каких следственных действиях она была бы эффективной?** | |
| | Допрос | 71 % |
| | Очная ставка | 68 % |
| | Предъявление для опознания | 54 % |
| | Иные | |
| 15 | **Считаете ли Вы целесообразным удостоверять процессуальные документы электронной подписью?** | |
| | Да, считаем это целесообразным и необходимым | 68 % |
| | Нет, это нецелесообразно | 32 % |
| | Иное | |

*Приложение 2*

## Перечень основных криминалистически значимых сведений из цифрового профиля гражданина России

| Источник данных | Тип данных, характер сведений |
|---|---|
| Министерство внутренних дел РФ | – паспорт и загранпаспорт;<br>– водительское удостоверение;<br>– свидетельство о регистрации транспортного средства;<br>– сведения из реестра транспортных средств;<br>– сведения по миграционному учету иностранных граждан, связанных с изучаемым гражданином РФ (приглашение иностранца, его регистрация, трудоустройство, оформление временного проживания или вида на жительство и т.п.);<br>– адресно-справочная информация;<br>– регистрация по месту жительства или пребывания;<br>– судимость, привлечение к уголовной, административной ответственности, наличие меры пресечения, отбывание наказания;<br>— история выданных паспортов |
| Росгвардия | – разрешение на приобретение оружия;<br>– наличие оружия;<br>– свидетельство частного охранника |
| Фонд пенсионного и социального страхования РФ | – СНИЛС;<br>– назначенные пенсии и социальные выплаты;<br>– трудовая деятельность;<br>– меры социальной поддержки;<br>– сведения из регистров материнского капитала;<br>– сведения об отнесении к категории граждан предпенсионного возраста;<br>– наличие нетрудоспособных родственников;<br>– информация о доставке пенсии и социальных выплат;<br>– сведения о детях;<br>– сведения о предоставлении путевок на санаторно-курортное лечение, бесплатного проезда;<br>– наличие технических средств и услуг для реабилитации |
| Федеральная налоговая служба | – ИНН;<br>– выписки из реестра плательщиков налогов; |

| | |
|---|---|
| | – справка 2-НДФЛ;<br>– декларация 3-НДФЛ;<br>– выписки ЕГРИП и ЕГРЮЛ;<br>– сведения о доходах и выплатах страховых взносов в пользу физлиц;<br>– сведения о самозанятости;<br>– сведения о зарегистрированной ККТ и адресах ее местонахождения;<br>– сведения, содержащиеся в государственном адресном реестре |
| Федеральный фонд обязательного медицинского страхования | – полис ОМС;<br>– сведения о прикреплении к медицинской организации;<br>– сведения об инвалидности |
| Федеральная служба государственной регистрации, кадастра и картографии | сведения об объектах недвижимости в собственности, в залоге, аренде и пр. |
| Органы записи актов гражданского состояния | – свидетельство о рождении;<br>– свидетельства о заключении и расторжении брака;<br>– свидетельство об установлении отцовства;<br>– свидетельство о смерти;<br>– сведения об усыновлении;<br>– наличие статуса многодетной семьи |
| Банк России | сведения из бюро кредитных историй (в каких банках, финансовых организациях и на какие цели брались кредиты, порядок их погашения) |
| Министерство спорта РФ | – сведения о сдаче ГТО;<br>– сведения о членстве в спортивной организации;<br>– наличие паспорта болельщика |
| Федеральная служба судебных приставов | информация о том, есть ли исполнительные производства и по каким обязательствам |