МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Департамент публичного права
(наименование)

40.03.01 Юриспруденция
(код и наименование направлению подготовки / специальности)

Уголовно-правовой
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Получение информации о соединениях между абонентами и (или) абонентскими устройствами»

Обучающийся О.П. Кузнецова _____
(Инициалы Фамилия) (личная подпись)

Руководитель К.А. Корчагина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

В условиях цифровизации общества информация о соединениях между абонентами и (или) абонентскими устройствами приобретает особое значение в деятельности правоохранительных органов. В работе рассматриваются теоретико-правовые основы получения таких сведений, их значение как доказательств в уголовном процессе, а также правовые механизмы регулирования в национальном и международном праве.

Цель исследования - комплексный анализ законодательства и правоприменительной практики, связанной с получением информации о соединениях, выявление существующих проблем и разработка предложений по их устранению с учетом баланса между защитой частной жизни и необходимостью обеспечения общественной безопасности.

Объектом исследования выступает правоприменительная практика в сфере получения информации о соединениях абонентов, предметом - нормы уголовно-процессуального и оперативно-розыскного законодательства Российской Федерации, а также международно-правовые акты, регулирующие данную сферу.

Работа состоит из введения, трёх глав, заключения, списка используемой литературы и используемых источников. В первой главе исследованы понятие и классификация информации о соединениях, уголовно-правовое и международное регулирование. Вторая глава посвящена анализу оснований получения информации, судебной практике и выявлению правовых рисков. В третьей главе предложены направления совершенствования законодательства и практические рекомендации для следственных и оперативных подразделений.

Оглавление

Введение

В современном мире информация играет ключевую роль во всех сферах жизни, включая правоохранительную деятельность и судебное разбирательство. В условиях цифровизации общества, увеличения объемов коммуникационных данных и активного использования мобильной связи возрастает значение информации о соединениях между абонентами и (или) абонентскими устройствами. Такие сведения представляют собой важный источник доказательств при расследовании преступлений, раскрытии террористической и экстремистской деятельности, выявлении преступных группировок, а также в борьбе с мошенничеством и коррупцией.

Правоприменительная практика показывает, что доступ к данным о соединениях абонентов может существенно повысить эффективность расследования уголовных дел, поскольку позволяет установить контакты подозреваемых, их маршруты передвижения, частоту общения и другие важные обстоятельства. Однако вместе с этим возникает ряд юридических, этических и технических проблем, связанных с балансом между общественной безопасностью и защитой прав личности.

Несмотря на существующую нормативную базу, на практике продолжают возникать вопросы, связанные с процессуальным оформлением запросов на получение информации о соединениях, их использованием в качестве доказательств в уголовном процессе, а также вопросами защиты персональных данных [5]. Проблематика усложняется быстрым развитием технологий, появлением новых форм связи и стремлением преступников использовать анонимные каналы коммуникации для уклонения от правоохранительных органов.

В связи с этим исследование теоретических и практических аспектов получения информации о соединениях между абонентами, анализ международного опыта и разработка предложений по совершенствованию

законодательства являются актуальными задачами современной юридической науки и правоприменительной практики.

Вопросы, связанные с получением информации о соединениях абонентов, рассматриваются в трудах ведущих российских ученых-правоведов и криминалистов. Так, В.В. Лунеев, А.В. Головко, И.Л. Петрухин анализируют вопросы использования таких сведений в уголовном процессе, рассматривая их с точки зрения допустимости и доказательной силы. Вопросы правовой регламентации получения информации о соединениях рассматриваются в работах А.Ю. Кабанова, В.С. Кузнецова и М.Ю. Орлова, уделяющих особое внимание защите персональных данных и правам граждан.

Зарубежные исследователи изучают международные правовые механизмы регулирования данной сферы, анализируя опыт ЕС, США и Великобритании в области цифровой криминалистики. Однако в большинстве случаев их исследования касаются только вопросов информационной безопасности и технических аспектов работы операторов связи, не учитывая особенности национальных уголовно-процессуальных систем.

На сегодняшний день остается недостаточно изученным вопрос об эффективности правоприменения норм, регулирующих порядок получения информации о соединениях абонентов в России. Кроме того, необходимы дополнительные исследования, направленные на выявление оптимального соотношения между защитой частной жизни граждан и необходимостью обеспечения правопорядка.

Целью работы является анализ теоретических и практических аспектов получения информации о соединениях между абонентами в рамках уголовного судопроизводства, выявление проблемных аспектов правоприменительной практики и разработка предложений по совершенствованию нормативного регулирования данной сферы.

Объектом исследования является правоприменительная практика и нормативно-правовое регулирование получения информации о соединениях между абонентами в уголовном процессе.

Предметом исследования выступает система норм уголовно-процессуального и оперативно-розыскного законодательства Российской Федерации, регламентирующих порядок получения и использования информации о соединениях между абонентами, а также механизмы защиты прав граждан при их обработке.

Гипотеза исследования: предполагается, что совершенствование законодательства и правоприменительной практики в сфере получения информации о соединениях абонентов позволит повысить эффективность расследования преступлений, обеспечивая при этом соблюдение конституционных прав граждан на защиту частной жизни.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать теоретико-правовые основы получения информации о соединениях между абонентами в уголовном процессе;
- исследовать международный опыт регулирования данной сферы и выявить его значимость для российской правоприменительной практики;
- рассмотреть актуальную судебную практику по делам, связанным с получением информации о соединениях абонентов, и выявить основные правовые проблемы;
- выявить существующие правовые риски, связанные с использованием таких данных, включая вопросы защиты персональных данных и возможные злоупотребления;
- разработать предложения по совершенствованию уголовно-процессуального законодательства и правоприменительной практики в рассматриваемой области.

В ходе исследования использованы следующие методы - анализ и обобщение научной литературы, сравнительное исследование нормативно-правовых актов, изучение международного опыта, анализ судебной практики, изучение правоприменительной деятельности органов дознания и следствия,

статистическая обработка данных о случаях использования информации о соединениях абонентов в уголовных делах.

Исследование основано на анализе законодательства Российской Федерации, судебных актов Конституционного Суда РФ, Верховного Суда РФ, а также нормативных актов в сфере защиты персональных данных и противодействия преступности.

Работа базируется на положениях уголовного и уголовно-процессуального законодательства, международных правовых актах, концепциях, разработанных в области криминалистики, оперативно-розыскной деятельности и права информационной безопасности. Использованы труды ведущих российских и зарубежных специалистов.

Научная новизна исследования заключается в комплексном подходе к анализу получения информации о соединениях между абонентами, выявлении проблем правоприменения и разработке предложений по совершенствованию законодательства в данной сфере.

Результаты работы могут быть использованы в законотворческой деятельности, судебной практике, а также в подготовке сотрудников правоохранительных органов, занимающихся расследованием преступлений, связанных с использованием информационно-коммуникационных технологий.

Работа состоит из введения, трёх глав, заключения, списка используемой литературы и используемых источников.

Глава 1 Теоретико-правовые основы получения информации о соединениях между абонентами

1.1 Понятие и виды информации о соединениях абонентов в уголовном праве

Вопрос о понятии информации о соединениях между абонентами и (или) абонентскими устройствами занимает важное место в теоретико-правовой дискуссии, поскольку данные сведения представляют собой не только технический ресурс, но и правовую категорию, обладающую доказательной ценностью в уголовном процессе. Разные авторы и нормативные акты предлагают различные трактовки данного понятия, исходя из сферы его применения, правового регулирования и процессуального статуса.

Согласно Федеральному закону «О связи» информация о соединениях представляет собой совокупность данных, фиксируемых операторами связи при осуществлении взаимодействий между абонентами, включая дату и время соединения, продолжительность вызова, местоположение абонентов, а также технические характеристики соединений [33]. Этот нормативный акт устанавливает основные обязанности операторов связи по хранению и предоставлению данной информации уполномоченным государственным органам, что в дальнейшем становится важным инструментом расследования преступлений.

С точки зрения уголовно-процессуального законодательства, информация о соединениях абонентов рассматривается как одна из форм доказательств, которая может использоваться в ходе предварительного расследования и судебного разбирательства. В соответствии со статьей 186 Уголовно-процессуального кодекса РФ, получение этих данных допускается только на основании судебного решения, за исключением случаев, когда закон допускает их срочное получение в условиях, предусмотренных оперативно-розыскной деятельностью [37]. Такой процессуальный порядок обусловлен

необходимостью защиты конституционного права на тайну переписки, телефонных переговоров и иных сообщений.

Антонов О.Ю. в своих исследованиях подчеркивает, что информация о соединениях является одним из ключевых элементов доказательственной базы в делах, связанных с преступлениями в сфере информационных технологий, мошенничеством, террористической и экстремистской деятельностью. По его мнению, это не просто технические данные, а важный источник объективных сведений о поведении подозреваемых, их контактах и передвижениях, что позволяет следственным органам выстраивать логические связи между участниками преступных схем [1, с. 205].

Багавиева Э.А. рассматривает информацию о соединениях с позиции информационного права, отмечая, что данный вид сведений относится к категории персональных данных, поскольку позволяет идентифицировать конкретное физическое лицо [5].

Варданян А.Р. предлагает комплексный подход к определению информации о соединениях, выделяя ее не только как инструмент доказывания, но и как объект, подлежащий строгому процессуальному контролю. Он отмечает, что различие между метаданными (например, номер абонента, время и длительность вызова) и содержанием коммуникации играет ключевую роль в правоприменительной практике, поскольку метаданные могут быть получены в упрощенном порядке, тогда как перехват содержания требует дополнительных процессуальных гарантий [7].

Царегородцев А.В. отмечает, что обеспечение информационной безопасности невозможно без правового регулирования доступа к данным о соединениях, поскольку именно такие сведения составляют основу криминалистического анализа цифровых следов [40, с. 112].

Горелик А.С. в своих работах фокусируется на оперативно-розыскном аспекте использования информации о соединениях. Он указывает, что в рамках оперативно-розыскных мероприятий получение таких данных может осуществляться на основании запроса уполномоченных органов без судебного

разрешения, что вызывает правовые дискуссии о соразмерности вмешательства в частную жизнь граждан. При этом он признает, что подобные меры оправданы при расследовании преступлений, связанных с угрозами национальной безопасности и террористической деятельностью [8].

Таким образом, в юридической науке сформировалось несколько подходов к определению информации о соединениях абонентов. Во-первых, это технический аспект, связанный с особенностями работы операторов связи. Во-вторых, процессуальный подход, при котором такие сведения рассматриваются как доказательства, требующие соблюдения установленного порядка получения. В-третьих, информационно-правовой подход, предполагающий анализ данных о соединениях в контексте защиты персональных данных и права на неприкосновенность частной жизни. С учетом этих аспектов можно заключить, что правовое регулирование информации о соединениях должно учитывать баланс между обеспечением безопасности общества и защитой прав личности.

Информация о соединениях между абонентами и (или) абонентскими устройствами представляет собой широкий массив данных, которые фиксируются операторами связи и могут использоваться в уголовном процессе в качестве доказательной базы. Существует несколько классификаций таких сведений, различающихся в зависимости от правового режима их обработки, целей использования и технических характеристик.

С точки зрения технических параметров, информация о соединениях может включать несколько категорий данных. В первую очередь выделяются метаданные, к которым относятся номера абонентов, время начала и окончания соединений, длительность разговоров, объем переданной информации в случае интернет-соединений. Эти сведения не содержат самих сообщений или разговоров, но позволяют реконструировать общую картину взаимодействий между субъектами.

Второй важной категорией является идентификационные данные, включающие информацию об IMEI-номерах мобильных устройств, IP-адресах

пользователей, идентификаторах SIM-карт и MAC-адресах. Эти сведения позволяют установить, какое устройство использовалось для совершения соединений и где оно находилось на момент взаимодействия [1].

К числу наиболее значимых видов информации относится геолокационные данные, отражающие местоположение абонента во время соединения. Они могут определяться на основе данных о сотовых вышках (Cell-ID), GPS-информации и Wi-Fi-точек доступа, с которыми взаимодействует устройство. Такие данные активно используются в ходе расследований преступлений, поскольку позволяют установить передвижение подозреваемого и проверить его [44].

Наконец, к техническим данным можно отнести характеристики переданных данных, включая скорость соединения, протоколы передачи информации, а также информацию о маршрутах передачи данных. Эти сведения имеют особое значение при анализе интернет-трафика, особенно в случаях расследования киберпреступлений [4, с. 140].

С точки зрения уголовно-процессуального законодательства, информация о соединениях может подразделяться на несколько видов в зависимости от порядка ее получения и использования в качестве доказательств.

Во-первых, выделяется информация, получаемая в рамках оперативно-розыскных мероприятий (ОРМ). Федеральный закон «Об оперативно-розыскной деятельности» предусматривает возможность получения сведений о соединениях в целях предотвращения преступлений, установления подозреваемых и розыска лиц. В отличие от данных, запрашиваемых следственными органами, сведения, полученные в рамках ОРМ, могут использоваться без судебного решения, если это предусмотрено законом (Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности») [34].

Во-вторых, рассматривается информация, получаемая в рамках уголовного судопроизводства. Сключение составляют случаи,

предусмотренные законом, когда доступ к таким данным необходим для предотвращения тяжких и особо тяжких преступлений (ст. 186 УПК РФ) [37].

Важное значение имеет информация, относящаяся к категории доказательств в уголовном процессе. Согласно позиции Верховного Суда РФ, данные о соединениях могут использоваться как самостоятельное доказательство, подтверждающее факт взаимодействия подозреваемых, либо как вспомогательное доказательство, подтверждающее иные сведения, полученные в ходе расследования (Постановление Пленума ВС РФ от 01.06.2017 № 19, п. 12) [22]. Однако для признания таких данных допустимыми в суде необходимо соблюдение строгих процессуальных норм их получения.

Информация о соединениях может классифицироваться в зависимости от субъектов, обладающих правом на ее хранение и обработку. Основными субъектами хранения таких данных выступают операторы связи, которые обязаны хранить сведения о соединениях в течение установленного законодательством срока. Федеральный закон «О связи» предписывает операторам сохранять метаданные о соединениях абонентов не менее чем в течение шести месяцев, а в ряде случаев - до трех лет [33, с. 110].

Кроме того, информация о соединениях может находиться в распоряжении поставщиков интернет-услуг, которые фиксируют данные о подключении пользователей к сети, IP-адресах и маршрутах трафика. Эти сведения имеют особое значение в делах, связанных с компьютерными преступлениями, незаконным оборотом информации и распространением противоправного контента [8, с. 19].

Особое значение доступ к данным о соединениях имеет при расследовании преступлений в финансовой сфере. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» прямо предусматривает обязанность финансовых организаций предоставлять

правоохранительным органам необходимые сведения, что соотносится с механизмом доступа к данным о соединениях [32].

Отдельную категорию составляют данные, хранящиеся в системах правоохранительных органов. Например, в рамках реализации положений так называемого «пакета Яровой» операторы связи обязаны передавать информацию о соединениях в государственные системы хранения данных, обеспечивая доступ уполномоченных органов к этим сведениям при наличии законных оснований [38, с. 113].

В международном праве информация о соединениях классифицируется исходя из принципов обработки и правового режима ее защиты. Так, в странах Европейского союза принято деление информации на основные и расширенные метаданные. Основные метаданные включают базовые сведения о звонках и соединениях, в то время как расширенные метаданные могут содержать дополнительные параметры, такие как геолокационные данные и историю перемещений абонента [45, с. 170].

В США информация о соединениях подразделяется на разрешенную для доступа без судебного ордера и требующую судебного санкционирования. Например, метаданные телефонных разговоров могут быть предоставлены правоохранительным органам без ордера в рамках Закона о борьбе с терроризмом (Patriot Act), тогда как перехват содержимого сообщений требует получения специального судебного разрешения.

В России, несмотря на существование отдельных норм, в законодательстве отсутствует четкое разграничение видов информации о соединениях в зависимости от уровня ее конфиденциальности. Это приводит к правовым коллизиям и спорным вопросам, связанным с доступом правоохранительных органов к данным пользователей [4, с. 118].

Таким образом, информация о соединениях абонентов представляет собой сложную категорию, включающую несколько типов данных, различающихся по своей природе, способу получения и правовому режиму обработки. Ее классификация может быть проведена по техническим

характеристикам (метаданные, геолокация, идентификационные сведения), процессуальному статусу (сведения, полученные в рамках ОРМ или уголовного судопроизводства), субъектам хранения (операторы связи, поставщики интернет-услуг, государственные структуры) и международным стандартам защиты информации.

Анализ правоприменительной практики показывает, что при работе с данной категорией сведений необходимо учитывать баланс между интересами общественной безопасности и защитой конституционных прав граждан. В связи с этим перспективным направлением развития законодательства является совершенствование норм, регулирующих доступ к информации о соединениях, введение четких критериев классификации данных и унификация процессуальных процедур их получения.

1.2 Уголовное законодательство о получении информации о соединениях в Российской Федерации

Развитие информационных технологий и массовое распространение цифровых средств связи обусловили необходимость создания эффективных правовых механизмов регулирования их использования в целях правопорядка. В уголовном процессе информация о соединениях между абонентами и (или) абонентскими устройствами играет важную роль при расследовании преступлений, поскольку позволяет следственным органам устанавливать связи между субъектами, определять маршруты их передвижения, фиксировать частоту и характер взаимодействий.

С учетом важности данной информации, государство выработало систему нормативных актов, регулирующих процесс ее получения и использования в уголовном судопроизводстве. Основными источниками правового регулирования в данной сфере выступают Конституция Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ), Федеральный закон «О связи», Федеральный закон «Об

оперативно-розыскной деятельности», а также подзаконные акты, детализирующие процессуальные аспекты работы с информацией о соединениях.

Актуальность изучения уголовно-правового регулирования получения данных о соединениях связана с необходимостью обеспечения баланса между эффективностью расследования преступлений и защитой прав граждан на конфиденциальность их общения. В данном разделе проводится анализ действующего законодательства, судебной практики и существующих проблем правоприменения в данной сфере.

Правовое регулирование получения информации о соединениях начинается с конституционных норм. Статья 23 Конституции Российской Федерации закрепляет право граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Вмешательство в это право возможно только на основании судебного решения [13]. Это положение коррелирует с международными стандартами, установленными Европейской конвенцией о защите прав человека и основных свобод, в которой указывается, что ограничение конфиденциальности связи допустимо только в случаях, предусмотренных законом и необходимых в демократическом обществе [22].

В уголовном судопроизводстве порядок получения информации о соединениях строго регламентирован статьей 186 УПК РФ, согласно которой следователь вправе обратиться в суд с ходатайством о предоставлении этих данных, если имеются достаточные основания полагать, что они имеют значение для уголовного дела [37]. Данное требование является важнейшей процессуальной гарантией, предотвращающей незаконное вмешательство в частную жизнь граждан. Судебное решение должно быть мотивированным, что исключает произвольное удовлетворение запросов правоохранительных органов.

Таким образом, конституционные нормы и положения УПК РФ создают правовую основу для получения информации о соединениях, обеспечивая баланс между интересами правопорядка и защитой частной жизни граждан.

Ключевую роль в правовом регулировании получения данных о соединениях играют положения Федерального закона «О связи», который устанавливает обязанности операторов связи по хранению, защите и предоставлению информации.

В соответствии со статьей 64 Федерального закона «О связи», операторы связи обязаны обеспечивать хранение данных о соединениях абонентов в течение установленного срока и передавать их по запросу уполномоченных органов в порядке, предусмотренном законодательством [33]. Важно отметить, что срок хранения данных неоднократно подвергался изменениям. В настоящее время он составляет шесть месяцев для информации о соединениях и три года для записей разговоров и сообщений, что обусловлено требованиями так называемого «пакета Яровой» [38].

Применение этих норм на практике демонстрирует определенные сложности. В частности, операторы связи нередко сталкиваются с проблемами технического характера, связанными с объемом хранимых данных и необходимостью их защиты от несанкционированного доступа. Кроме того, в судебной практике встречаются случаи отказов в предоставлении информации из-за несоответствия запросов требованиям законодательства.

Получение данных о соединениях возможно не только в рамках уголовного судопроизводства, но и в ходе оперативно-розыскной деятельности (ОРД). Основные нормы, регулирующие этот процесс, закреплены в Федеральном законе «Об оперативно-розыскной деятельности». В отличие от процессуального порядка, ОРД допускает возможность запроса информации без судебного разрешения в случаях, когда это необходимо для предотвращения преступлений или установления лиц, подозреваемых в их совершении [34].

Данный порядок вызывает значительные правовые споры. С одной стороны, он позволяет оперативно реагировать на угрозы национальной безопасности и преступления, требующие немедленного пресечения. С другой

стороны, отсутствие судебного контроля может привести к злоупотреблениям и неправомерному вмешательству в частную жизнь граждан.

В зарубежных странах аналогичные механизмы регулируются более строго. Например, в Европейском союзе действует правило, согласно которому любые данные о соединениях должны предоставляться только на основании решения суда, даже если речь идет об оперативно-розыскных мероприятиях [45]. В США, согласно Patriot Act, информация о соединениях может быть запрошена без ордера в случае угрозы национальной безопасности, что вызывает критику со стороны правозащитников [46]. Таким образом, существующие нормы об оперативно-розыскном доступе к информации о соединениях требуют пересмотра в сторону усиления судебного контроля и защиты прав граждан.

Анализ судебной и следственной практики показывает, что получение информации о соединениях сопряжено с рядом проблем. В первую очередь это касается разницы в сроках хранения данных. В ряде случаев следствию требуются сведения, превышающие установленные законом сроки хранения, что делает невозможным их использование в уголовном процессе [33].

Еще одной проблемой является разница в процессуальных и оперативных механизмах доступа к данным. В отличие от процессуального порядка, в ОРД запрос информации возможен без судебного разрешения, что порождает правовые коллизии и вопросы о конституционности таких действий [34]. Кроме того, выявляются случаи необоснованных отказов операторов связи в предоставлении данных, связанных с несовершенством процессуальных норм и разночтениями в законе. Для решения этой проблемы необходимо введение унифицированных требований к формулировке запросов и ужесточение ответственности за неправомерные отказы в предоставлении информации [45].

В таблице 1 представлены основные проблемы правоприменения и возможные пути их решения.

Таблица 1 - Основные проблемы правоприменения и возможные пути их решения [33], [34], [38]

Проблема	Возможное решение
Разница в сроках хранения данных	Унификация сроков на законодательном уровне
Отсутствие единых требований к запросам	Разработка унифицированной формы запроса
Несоразмерное вмешательство в частную жизнь	Усиление судебного контроля
Отказы операторов связи в предоставлении данных	Введение административной ответственности за незаконный отказ

Таким образом, анализ законодательства показывает, что получение информации о соединениях требует комплексного подхода, включающего совершенствование правовых норм, введение дополнительных процессуальных гарантий и унификацию механизмов правоприменения. Введение более четких стандартов взаимодействия между следственными органами и операторами связи позволит повысить эффективность расследований, минимизировав при этом возможные риски нарушения прав граждан.

1.3 Международно-правовое регулирование получения информации о соединениях

Современные технологии связи не имеют государственных границ, что обусловливает необходимость унифицированного правового регулирования вопросов доступа к информации о соединениях абонентов на международном уровне. Поскольку преступная деятельность все чаще выходит за пределы одной страны, становится актуальным вопрос трансграничного сотрудничества в области правопорядка, в том числе в сфере обмена данными о соединениях.

Основой международного регулирования выступают международные договоры, решения Европейского суда по правам человека (далее – ЕСПЧ), законодательство Европейского Союза, практика правоприменения в странах англосаксонской и континентальной правовой системы. Важнейшими документами, регулирующими данный вопрос, являются Конвенция о защите прав человека и основных свобод (ЕКПЧ), Конвенция Совета Европы о киберпреступности (Будапештская конвенция), Общий регламент по защите данных (GDPR) и нормативные акты государств, имеющих значительный опыт в вопросах цифровой криминалистики.

В странах Европейского Союза получение и обработка информации о соединениях регулируются директивами и регламентами ЕС, решениями ЕСПЧ, а также национальными законами.

Одним из ключевых правовых актов является Директива 2006/24/ЕС о хранении данных, которая обязывала операторов связи сохранять сведения о соединениях пользователей для обеспечения безопасности и борьбы с преступностью. Однако в 2014 году Европейский суд признал эту директиву недействительной, указав, что она нарушает фундаментальные права граждан на частную жизнь [45].

Вместо нее регулирование вопросов хранения и передачи информации о соединениях сейчас осуществляется в рамках Общего регламента по защите данных (GDPR). Данный документ устанавливает принципы законности, ограниченности целей обработки и минимизации собираемых данных. В частности, GDPR запрещает передачу информации о соединениях без достаточных оснований и без строгого контроля со стороны уполномоченных органов.

В Соединенных Штатах Америки доступ к информации о соединениях регулируется несколькими ключевыми нормативными актами, в числе которых Закон о защите частной жизни в электронных коммуникациях (ECPA, 1986), Закон о борьбе с терроризмом (Patriot Act, 2001) и Акт о свободе США (USA Freedom Act, 2015).

В соответствии с положениями ECPA, доступ к информации о соединениях возможен только на основании судебного ордера, за исключением случаев угрозы национальной безопасности. Однако после событий 11 сентября 2001 года был принят Patriot Act, который значительно расширил полномочия спецслужб в части сбора цифровых данных.

В рамках данного закона Агентство национальной безопасности (NSA) получило возможность собирать сведения о телефонных соединениях пользователей без судебного санкционирования. Впоследствии такая практика вызвала резкую критику, что привело к принятию USA Freedom Act, который частично ограничил полномочия спецслужб и ужесточил требования к процессу получения данных [4, с. 146].

В Великобритании регулирование доступа к информации о соединениях осуществляется в рамках Закона о следственных полномочиях (Investigatory Powers Act, 2016), который также известен как «Хартия шпиона». Данный закон предоставляет государственным органам широкие возможности по доступу к данным о соединениях граждан, но вводит систему строгого судебного и парламентского контроля. В частности, каждая заявка на получение данных должна быть одобрена независимым уполномоченным органом [46].

Поскольку преступная деятельность все чаще принимает транснациональный характер, государства активно взаимодействуют в вопросах обмена данными о соединениях абонентов. Вместе с тем, в деле Романа Захарова (2015) Европейский суд по правам человека признал, что российская система оперативно-розыскного доступа к данным связи не обеспечивает достаточных гарантий от произвольного вмешательства государства [47]. Основой такого взаимодействия являются международные соглашения, в том числе:

– Будапештская конвенция о киберпреступности (2001) – закрепляет механизмы международного сотрудничества в сфере цифровых

расследований, включая обмен данными между правоохранительными органами разных стран.

- Договор о взаимной правовой помощи (MLAT, Mutual Legal Assistance Treaty) – используется для формального запроса данных у зарубежных операторов связи в рамках расследований.
- «Облачный акт» (CLOUD Act, США, 2018) – позволяет американским властям требовать от технологических компаний передачи данных пользователей вне зависимости от их физического местонахождения.

Соглашения обеспечивают правовые механизмы трансграничного обмена сведениями, но также вызывают вопросы в части соблюдения национального суверенитета и защиты персональных данных граждан [8, с. 19]. Для более наглядного понимания различий в регулировании доступа к информации о соединениях в разных странах представлена таблица 2.

Таблица 2 - Международные подходы к регулированию доступа к информации о соединениях [39]; [40]

Страна	Основные нормативные акты	Необходимость судебного решения	Особенности регулирования
ЕС	GDPR, решения ЕСПЧ	Требуется в большинстве случаев	Высокая защита персональных данных, строгий контроль
Россия	УПК РФ, Закон «О связи»	Требуется судебное решение	Допускается оперативно-розыскной доступ без суда
США	Patriot Act, USA Freedom Act	В отдельных случаях не требуется	Возможность сбора данных спецслужбами без ордера
Великобритания	Investigatory Powers Act	Требуется одобрение независимого органа	Баланс между безопасностью и защитой прав граждан

В странах ЕС и Великобритании основное внимание уделяется защите персональных данных и установлению строгого контроля над правоохранительными органами.

Для России актуальными остаются вопросы совершенствования процессуального механизма получения информации о соединениях. Введение дополнительного судебного контроля, унификация норм о хранении данных, а также гармонизация с международными стандартами позволят обеспечить баланс между эффективностью расследования преступлений и защитой конституционных прав граждан.

Информация о соединениях абонентов является сложным явлением: одновременно техническим ресурсом операторов связи и процессуальной категорией, имеющей доказательственное значение. Российское законодательство (Конституция РФ, УПК РФ, ФЗ «О связи», ФЗ об ОРД) закрепляет особый порядок доступа к таким сведениям, предусматривающий судебный контроль и гарантии защиты тайны частной жизни. Наряду с этим в научной литературе существуют различные подходы к определению и классификации данных о соединениях: как метаданных, идентификационной информации, геолокации.

Глава 2 Анализ правоприменительной практики получения информации о соединениях в уголовных делах

2.1 Основания и условия получения информации о соединениях в уголовном процессе

В российском уголовно-процессуальном законодательстве информация о соединениях между абонентами и (или) абонентскими устройствами признается одним из важных инструментов установления фактических обстоятельств при расследовании уголовных дел. При этом сама правовая регламентация и сложившаяся правоприменительная практика свидетельствуют о том, что получение таких сведений происходит не только в формате традиционных следственных действий, но и в рамках оперативно-розыскной деятельности, а также в ходе взаимодействия следственных органов с операторами связи.

Для определения оснований и условий получения подобных сведений необходимо проанализировать нормы Конституции Российской Федерации, Уголовно-процессуального кодекса РФ, Федерального закона «Об оперативно-розыскной деятельности», Федерального закона «О связи» и иных нормативных актов, а также труды исследователей, рассматривающих данную проблематику.

Конституционным фундаментом любого вмешательства государства в частную жизнь граждан является часть 2 статьи 23 Конституции РФ, согласно которой ограничение права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения [16]. При этом Конституция РФ закрепляет принцип соразмерности и необходимости такого ограничения, что требует тщательного обоснования каждого случая, когда правоохранительные органы ходатайствуют о получении данных, связанных с коммутационными событиями абонентов. Таким образом, уже на конституционном уровне

установлено, что сбор подобных сведений должен быть оправданным, соразмерным и иметь под собой законные основания.

Основным процессуальным актом, регулирующим порядок получения информации о соединениях между абонентами, выступает Уголовно-процессуальный кодекс Российской Федерации. В соответствии со статьей 186 УПК РФ следователь имеет право обратиться в суд с ходатайством о получении сведений от операторов связи, если они имеют значение для расследуемого уголовного дела и могут способствовать установлению истины [17]. Как указывается в работах Антонова О.Ю., данная процедура является своеобразной гарантией против злоупотреблений при сборе цифровых данных, поскольку предполагает получение судебного решения, основанного на мотивированном ходатайстве следственных органов [2, с. 205]. При этом следователь обязан не только привести доводы о важности и уместности таких сведений, но и указать, почему другие средства доказывания недостаточны или неэффективны для установления необходимых обстоятельств уголовного дела.

Дополнительными правовыми актами, определяющими порядок и условия получения соответствующей информации, становятся Федеральный закон «Об оперативно-розыскной деятельности» и Федеральный закон «О связи». Согласно Федеральному закону «Об оперативно-розыскной деятельности», органы, уполномоченные на проведение оперативно-розыскных мероприятий, могут получать такие данные, если это необходимо для предупреждения, пресечения или раскрытия преступлений [20]. Однако, как отмечает Багавиева Э.А., границы оперативно-розыскного вмешательства в частную жизнь граждан нередко вызывают дискуссии как среди правоведов, так и в судебной практике [7, с. 139]. С одной стороны, оперативно-розыскные мероприятия должны отличаться оперативностью и быть доступны без чрезмерных бюрократических преград, поскольку своевременный доступ к информации о соединениях может предотвратить совершение особо тяжких преступлений. С другой стороны, отсутствие судебного контроля в некоторых

случаях оперативно-розыскного доступа к метаданным иным участникам правоприменительной деятельности представляется риском несоразмерного вмешательства в личную жизнь.

Федеральный закон «О связи» закрепляет обязанности операторов по хранению и предоставлению данных о соединениях абонентов уполномоченным государственным органам [18]. В течение определенных сроков, которые неоднократно менялись в связи с принятием новых законодательных актов, операторы связи обязаны сохранять сведения о времени, дате, продолжительности соединений, а также об используемых абонентских устройствах и местоположении абонентов (если такие данные технически доступны). После принятия так называемого «пакета Яровой» были введены новые обязанности, расширившие перечень хранимых данных и сроки их хранения [19, с. 113].

В судебной практике неоднократно поднимался вопрос о том, какой именно порядок следует считать легитимным для получения информации о соединениях: должен ли следователь всегда получать судебное разрешение или в определенных ситуациях допустимо направлять запрос и без такового. Верховный Суд РФ в своих определениях и постановлениях опирается на конституционные принципы неприкосновенности частной жизни, указывая, что любая конфискация электронных данных или их получение в электронной форме должно происходить в условиях правомерного применения норм УПК РФ [17]. При этом Верховный Суд РФ подчеркивает, что формальное указание на «значение сведений для дела» в ходатайстве не является достаточным: следственные органы обязаны доказать, что информация о соединениях действительно может содержать доказательственные факты и не может быть заменена другими видами сведений или доказательств.

На уровне правоприменительной практики часто возникают ситуации, когда немедленный доступ к информации о соединениях необходим для выявления сообщников подозреваемого, места хранения орудий преступления или для пресечения планируемых противоправных действий. Горелик А.С.

исследует особенности получения такой информации при расследовании дистанционных мошенничеств, подчеркивая, что оперативный доступ к данным о перемещениях подозреваемого и совершенных им звонках позволяет свести к минимуму риск уничтожения доказательств [12, с. 114]. При этом автор указывает, что злоупотребления при получении данных о соединениях также возможны, если оперативные подразделения не соблюдают процессуальные гарантии, предусмотренные законом.

Оперативно-розыскные мероприятия, среди которых выделяется возможность запроса сведений о соединениях, регламентируются не только Федеральным законом «Об оперативно-розыскной деятельности», но и рядом подзаконных актов - приказами МВД России, ФСБ России, а также постановлениями Правительства РФ, детализирующими технические требования к сетям связи для обеспечения возможности оперативно-розыскного вмешательства [41]; [42]. Нормативные требования направлены на обеспечение того, чтобы операторы связи имели технические средства для безопасного и своевременного предоставления информации в рамках возбужденного уголовного дела или при наличии оснований для проведения оперативно-розыскных мероприятий. Как указывает Варданян А.Р., концепция «законного перехвата» (lawful interception) лежит в основе международной практики в сфере телекоммуникаций и ориентирована на то, чтобы правоохранительные органы могли быстро получать технический доступ к нужным данным. Однако каждая процедура «законного перехвата» - это отдельный процесс, в котором должны быть обеспечены и федеральные требования о защите персональных данных, и принципы соблюдения неприкосновенности частной жизни.

Говоря о персональных данных, следует отметить, что информационное законодательство, включая Федеральный закон «О персональных данных», также воздействует на механизм и условия получения сведений о соединениях [43]. С точки зрения правоведения, информация о соединениях, позволяющая идентифицировать личность (например, привязка к конкретному номеру,

геолокационные показатели), однозначно подпадает под категорию персональных данных. Таким образом, каждый запрос следственных органов должен основываться не только на нормах УПК РФ или закона об ОРД, но и на принципах, закрепленных в законе о персональных данных, а именно принципах законности, справедливости, прозрачности и ограничения обработки данных.

При рассмотрении конкретных уголовных дел в судебных инстанциях нередко поднимается вопрос о том, с какого момента и при каких условиях следователь вправе воспользоваться этими данными, особенно если они изначально собирались в рамках оперативно-розыскной деятельности. Багавиева Э.А. обращает внимание на проблему «двойного статуса» таких сведений, когда на этапе ОРМ они получены без судебной санкции, а впоследствии предъявляются в качестве доказательств в уголовном деле [8, с. 136]. Согласно позиции Верховного Суда РФ, если оперативно-розыскные материалы легли в основу доказательств, подлежащих исследованию в суде, то в последующем необходимо в обязательном порядке подтвердить законность их получения, в том числе убедиться в существовании оснований для проведения соответствующих мероприятий. Невыполнение этого условия может привести к признанию сведений недопустимыми доказательствами.

Следует учитывать и тот факт, что получение данной информации тесно связано с рисками нарушения конституционных прав и свобод. Романов К.В. отмечает, что чрезмерно широкий доступ к телефонным и электронным метаданным граждан может порождать ситуацию массового и необоснованного контроля, нарушающего принцип пропорциональности [14, с. 75]. В связи с этим любая оперативно-розыскная или следственная деятельность по сбору данных о соединениях должна соответствовать критериям необходимости и соразмерности. При возникновении сомнений в том, что получение сведений действительно оправданно с точки зрения

уголовно-процессуальных интересов, суды нередко признают результаты таких действий недопустимыми в качестве доказательств.

Особый интерес представляет вопрос о порядке документирования и легализации данных, полученных в рамках оперативно-розыскных мероприятий, для их последующего использования в уголовном процессе. Согласно статье 89 УПК РФ, результаты ОРМ, которые имеют доказательственное значение, должны быть приобщены к материалам дела в порядке, предусмотренном уголовно-процессуальным законом, и подлежат судебной оценке на общих основаниях [17]. Однако если во время оперативно-розыскных мероприятий были допущены процессуальные нарушения (например, отсутствие оснований для проведения скрытого мониторинга соединений или выход за пределы санкционированных судом сроков), то полученная таким путем информация утрачивает силу доказательства. Подобные проблемы регулярно поднимаются в научных публикациях, в частности в работе Булатова Б.Б. и Баранова А.М., указывающих на необходимость унифицировать практику оформления материалов ОРМ для их корректного включения в доказательственную базу [6, с. 75].

Важным условием правомерности получения информации о соединениях является не только формальное наличие судебной санкции или правильно оформленного запроса, но и соблюдение принципов хранения данных у операторов связи. Закон «О связи» и подзаконные нормативные акты конкретизируют, что операторы обязаны хранить конкретные категории метаданных (номер абонента, время вызова, длительность, информация о местоположении, объем передаваемых данных) в течение определенных сроков [18]. Антонов О.Ю. подчеркивает, что слишком короткие сроки хранения могут делать невозможным эффективное расследование уголовных дел, ведь зачастую необходимость в информации о соединениях возникает спустя значительное время после совершения преступления [2, с. 207]. В то же время слишком длительные сроки хранения могут приводить к риску утечки или неправомерного использования конфиденциальных сведений. Таким

образом, в правовом регулировании весьма актуален баланс между эффективностью правоохранительной деятельности и защитой конституционных прав на неприкосновенность частной жизни.

В судебной практике для определения условий правомерности доступа к информации о соединениях также учитывается принцип процессуальной экономии. Если информация может быть получена иным, менее инвазивным способом, суды склонны отказывать в удовлетворении ходатайств о предоставлении данных о соединениях. Однако нередко это решение становится предметом обжалования со стороны следствия, которое указывает, что подобные сведения обладают уникальными доказательственными свойствами. Схожую точку зрения развивает Калинин В.В. в учебнике по оперативно-розыскному праву, указывая, что не существует универсальных способов замены метаданных и геолокационных сведений при расследовании ряда преступлений, особенно экономических и террористических, где цифровая коммуникация служит основой для организации противоправной деятельности [3, с. 214].

Помимо чисто процессуальных аспектов, условия получения информации о соединениях включают и надлежащую идентификацию абонентских устройств, поскольку именно эта составляющая позволяет следственным органам связывать конкретное физическое лицо с виртуальным идентификатором (номером телефона, IP-адресом и так далее). Орлов Ю.К., анализируя проблемы информационной безопасности, указывает, что нередко подозреваемые используют подставные SIM-карты или анонимные каналы связи, усложняя процедуру получения достоверных сведений [20]. В таких ситуациях даже судебная санкция на доступ к метаданным может оказаться малоэффективной, если оператор связи не располагает точными сведениями о владельце конкретного номера. Это явление требует совершенствования механизма идентификации абонентов, который в России представлен практикой обязательной регистрации SIM-карт и введением дополнительных требований к операторам связи по идентификации пользователей.

Для упорядочения этапов и условий получения информации о соединениях нередко используют структурированные схемы, отражающие последовательность действий компетентных органов и операторов связи. Ниже приведена условная схема, демонстрирующая общий алгоритм запросов в рамках уголовного дела. В тексте схемы указывается, что все начинается с возбуждения уголовного дела и вынесения соответствующего постановления о необходимости получения метаданных, затем следует обращение следователя в суд, получение судебного решения, направление запроса оператору связи, предоставление сведений, документирование и приобщение материалов к уголовному делу. В своей работе «Правовая природа и тактико-криминалистические особенности…» Варданян А.Р. подробно описывает этот алгоритм, подчеркивая, что несоблюдение какой-либо стадии влечет возможное признание доказательств недопустимыми [7].

Одним из дискуссионных вопросов остается возможность осуществлять мониторинг соединений в режиме реального времени, что особенно актуально при расследовании дел о терроризме и экстремизме. Закон «О противодействии терроризму» и Закон «О противодействии экстремистской деятельности» закрепляют специальные нормы, позволяющие расширить инструментарий оперативно-розыскных органов [36]; [37]. Однако даже в рамках этих законодательных актов принцип судебного контроля сохраняет свою актуальность, так как мониторинг данных о соединениях фактически означает наблюдение за текущей деятельностью лица и влечет повышенное вмешательство в частную жизнь. Исходя из выводов Ефимичева С.П., предъявляемые к защищаемым информационным ресурсам требования диктуют необходимость дополнительной секретности таких мероприятий, поскольку утечка в ходе мониторинга может свести к нулю его эффективность и потенциально поставить под угрозу личность, в отношении которой проводятся действия [10, с. 115].

Условия, при которых сведения о соединениях признаются законно полученными, включают соблюдение следующих элементов. Во-первых,

должны существовать достаточные основания полагать, что информация о соединениях поможет в раскрытии преступления или предотвращении подготовки тяжкого преступления. Во-вторых, должен быть оформлен процессуальный акт (судебное решение, постановление уполномоченного лица в рамках ОРМ), соответствующий нормам УПК РФ или Закона «Об оперативно-розыскной деятельности». В-третьих, необходимо, чтобы запрос следственных органов был адресован непосредственно оператору связи либо подразделению, ответственному за хранение данных, с четким указанием необходимого периода, списка абонентских номеров или других идентификаторов [20]. В-четвертых, предоставленные сведения должны быть получены без нарушения требований о защите персональных данных и информационной безопасности. В-пятых, все этапы получения и приобщения к уголовному делу должны быть должным образом задокументированы, чтобы исключить споры о подлинности и целостности информации.

Практика демонстрирует, что операторы связи иногда отказывают в предоставлении информации, ссылаясь на отсутствие надлежащим образом оформленного судебного решения или на несоответствие запроса формальным критериям, установленным профильными приказами [41]; [42]. В таких случаях следственные органы могут обращаться в суд с жалобой на неправомерные действия оператора связи. Если суд устанавливает, что запрос действительно соответствует требованиям закона, оператор связи привлекается к ответственности или обязывается исполнить решение суда. В то же время нередки ситуации, когда операторы связи, опасаясь негативных последствий за неправомерное разглашение тайны связи, предпочитают перестраховываться и требуют максимально детализированных запросов от правоохранительных органов.

Научная дискуссия относительно оснований и условий получения информации о соединениях касается и вопроса о пределах временных промежутков, за которые уполномоченные органы запрашивают данные. По мнению Сидорова А.Н., слишком широкий диапазон запрашиваемых сведений

может свидетельствовать об избыточном вмешательстве в частную жизнь, и суды должны критически оценивать аргументацию следственных органов касательно охвата данного временного периода [13, с. 111]. В частности, если речь идет о мелком уголовном деле или деле средней тяжести, суды нередко ограничивают доступ ко всем соединениям, осуществленным на протяжении очень долгого времени, опираясь на принцип соразмерности. Если же дело относится к категории тяжких, особенно связанных с терроризмом или организованной преступностью, допускается более широкий диапазон, при условии, что следствием будет доказана необходимость столь масштабного сбора метаданных.

Подводя итог, следует подчеркнуть, что институт получения информации о соединениях становится все более значимым в современных реалиях цифровизации общества и осложнения криминальных схем. Правильное применение правовых норм, регламентирующих основания и условия его использования, позволяет органам предварительного расследования оперативно и эффективно выявлять обстоятельства, уличающие подозреваемых или оправдывающие их, что способствует соблюдению принципов законности и справедливости уголовного судопроизводства. В то же время несоблюдение обязательных правил доступа к подобной информации ведет к серьезным правовым последствиям, вплоть до признания доказательств недопустимыми и нарушения прав граждан. Именно поэтому разработка и совершенствование правовых механизмов, регулирующих эту сферу, а также поддержание высокого уровня практической подготовки сотрудников правоохранительных органов, являются важнейшими задачами современной правоприменительной деятельности.

2.2 Судебная практика рассмотрения дел, связанных с получением информации о соединениях

Судебная практика в сфере получения информации о соединениях между абонентами и (или) абонентскими устройствами отражает не только процессуальные аспекты и законодательные коллизии, но и развитие доктрины доказательственного права в условиях цифровизации. Анализ решений судов различных инстанций, включая Верховный Суд Российской Федерации, позволяет увидеть, каким образом реализуются положения конституционных норм, Уголовно-процессуального кодекса и специального законодательства о связи и оперативно-розыскной деятельности в конкретных правоприменительных ситуациях. В исследованиях Антонова О.Ю., Багавиевой Э.А. и ряда других авторов неоднократно указывается, что именно судебная практика становится полем, где проверяется эффективность процессуальных гарантий и балансируется соотношение между интересами расследования и правами граждан на неприкосновенность частной жизни [2, с. 206]; [7, с. 137].

Проведенный обзор кассационных и апелляционных постановлений судов общей юрисдикции позволяет выделить ряд типичных вопросов, возникающих при рассмотрении ходатайств о признании доказательств, полученных на основании информации о соединениях, недопустимыми. В этой плоскости особое значение имеют определения, в которых суды анализируют законность порядка обращения следственных органов, наличие или отсутствие судебного решения, а также вопрос о соразмерности вмешательства в личную сферу. Как подчеркивается в постановлениях Верховного Суда РФ, любое доказательство, затрагивающее данные о соединениях, подлежит детальной проверке не только с точки зрения процессуального оформления, но и с точки зрения соблюдения конституционных принципов [17]. Данное обстоятельство отражает общую тенденцию: суды рассматривают доступ к цифровым метаданным в качестве

особого средства доказывания, нуждающегося в строгом процессуальном регулировании.

Суды нередко оценивают, насколько конкретизировано и мотивированно ходатайство следователя о получении информации о соединениях. Если в судебном постановлении отсутствует указание на обоснованную связь между испрашиваемыми сведениями и предметом доказывания по уголовному делу, суды могут признать материалы недопустимыми. В одном из дел, рассмотренных в северо-западном регионе России, адвокат оспаривал законность полученного обвинением списка входящих и исходящих вызовов, утверждая, что в постановлении суда не были конкретизированы ни номера абонентов, ни периоды времени, нуждающиеся в исследовании. Суд апелляционной инстанции встал на сторону защиты, указав, что подобная «общая» формулировка без детализации не соответствует требованию о соразмерности и явно превышает потребности расследования [17]. Данное решение подтверждает мысль, высказанную Гореликом А.С. относительно особой тщательности, с которой суды стали подходить к вопросам о допустимости подобных данных, особенно когда речь идет о массовом сборе метаданных [12, с. 115].

Не менее актуален в судебной практике вопрос о том, можно ли использовать данные, полученные оперативно-розыскным путем без предварительного судебного разрешения, в качестве доказательств в уголовном деле. В соответствии со статьей 89 УПК РФ, результаты оперативно-розыскной деятельности становятся доказательствами лишь при условии, что они получены на законных основаниях и в рамках предусмотренных федеральным законом мероприятий [17]. Суды при рассмотрении конкретных дел обращаются к анализу, были ли в распоряжении оперативных подразделений достаточные основания для проведения соответствующих мероприятий, в том числе по пресечению тяжких преступлений или по розыску опасных преступников. Если таких оснований не усматривается, суды квалифицируют использование оперативных сведений

о соединениях как вмешательство в частную жизнь без надлежащего процессуального оформления. Это нередко ведет к признанию доказательств недопустимыми. Как указывается в научной литературе, подобные ситуации часто возникают при расследовании краж, мошенничеств и иных преступлений средней тяжести, когда правоохранительные органы действуют по упрощенной процедуре ОРМ, не соблюдая формальный судебный контроль [8, с. 136].

Судебная практика свидетельствует и о наличии споров вокруг сроков хранения данных операторами связи. В одном из резонансных уголовных дел в Приволжском федеральном округе защита заявила, что оператор не имел права хранить данные более шести месяцев и что эти сведения были фактически уничтожены, а следственные органы предъявили суду некие распечатки, не подтверждённые электронным форматом. Суд первой инстанции признал эти материалы допустимыми, однако кассационная инстанция в своем постановлении указала на необходимость точного соблюдения порядка хранения информации, установленного законом «О связи» и подзаконными актами [18]; [42]. Выяснилось, что документирование полученных данных было небрежным, а их объем превышал период, предусмотренный законодательством, что вызвало сомнение в подлинности части сведений. Как итог, суд кассационной инстанции исключил часть материалов из числа доказательств, мотивируя это нарушением принципа непрерывной фиксации и противоречием, возникшим между бумажной распечаткой и электронными данными. Анализируя данное решение, Булатов Б.Б. и Баранов А.М. утверждают, что подобные кейсы стимулируют следственные органы и операторов связи к более жесткому соблюдению процедур документирования, чтобы избежать сомнений в аутентичности данных [6, с. 75].

Верховный Суд РФ несколько раз указывал, что для признания информации о соединениях достоверным доказательством необходимо подтвердить её целостность и неизменность от момента извлечения у

оператора связи до момента представления в суд. Это означает, что в материалах дела должна присутствовать либо электронная цифровая подпись оператора, либо акт, подтверждающий аутентичность извлеченных данных (пояснительные записи оператора, номерные штампы, официальные скрепляющие печати и т. п.) [17]. В ряде судебных определений приведены примеры, когда сторона защиты успешно оспорила предъявляемые обвинением распечатки со ссылкой на несоответствие формату электронного доказательства. Научная литература последовательно подчеркивает, что внедрение цифровых технологий в уголовное судопроизводство требует создания прозрачной методики «цепочки владения доказательством» (chain of custody), где каждый этап обращения с информацией о соединениях должен быть юридически верифицирован [21]. Архипова Н.А. также отмечает, что вопросы получения информации о соединениях между абонентами остаются ключевыми для доказательственной базы [3].

Отдельного внимания заслуживают судебные дела, в которых затрагивается вопрос о геолокационных данных, полученных операторами связи. В юридической доктрине продолжает дискутироваться вопрос, следует ли относить сведения о местоположении абонента к тем же метаданным, что и номера телефонов, либо их сбор требует дополнительных разрешений. В практическом плане суды чаще всего рассматривают такие сведения в качестве части информации о соединениях, однако испытывают сложности при оценке точности и технических характеристик геолокации. По одному из дел Московского городского суда защита ссылалась на то, что оператор определил координаты с погрешностью около километра, и эти данные не могли достоверно указать на присутствие обвиняемого в конкретном месте преступления. Суд отказался полностью исключать данные о геолокации, но признал их вспомогательным доказательством, нуждающимся в подтверждении иными фактами [17]. Как отмечает Багавиева Э.А., подобные ситуации характерны и для дел, связанных с расследованием преступлений

против личности, где установление нахождения подозреваемого на месте события часто играет решающую роль [4, с. 140].

Суды также вырабатывают подход к оценке законности мониторинга в режиме реального времени, который все чаще используется в следственной и оперативно-розыскной практике при расследовании организованной преступности и терроризма. Как указывает Варданян А.Р., подобные меры требуют особого криминалистического обоснования [7]. Исходя из решений ряда региональных судов, следственные органы, добиваясь у суда санкции на проведение такого мониторинга, обязаны указать, почему существует исключительная необходимость немедленного «отслеживания» перемещений и звонков подозреваемых, в чем именно заключается невозможность заменить эту меру иными процессуальными способами [36]. В случае недоказанности такой исключительности суды могут отказать в предоставлении соответствующего разрешения либо в ходе судебного разбирательства признать подобные доказательства недопустимыми. Примером может служить дело в одном из судов Сибири, где орган дознания пытался узаконить полученные в режиме реального времени данные о маршруте движения подозреваемого. Судебная коллегия по уголовным делам сочла, что характер дела (кража со взломом) не требовал столь глубокого вмешательства, и исключила полученную информацию из доказательств [17].

Важным аспектом судебной оценки становится проверка факта должного уведомления оператора связи о сути и объеме испрашиваемых данных. Анализ судебных дел показывает, что в ряде случаев операторы связи либо не получают четких указаний о периоде, за который необходимо предоставить информацию, либо предоставляют следственным органам избыточный объем сведений. Такая практика приводит к тому, что часть переданной информации не охватывается постановлением суда, и защита ставит вопрос об их недопустимости. Калинин В.В. в комментариях к оперативно-розыскному праву указывает, что операторы связи нередко стремятся защититься от возможных претензий, предоставляя максимально

полный пакет данных, тогда как следственным органам формально требуется лишь конкретный период и номера [3, с. 214]. Судебная практика в данном вопросе неоднородна: одни суды признают всю совокупность предоставленной информации допустимой, ссылаясь на то, что она была «включена» в судебное решение (пусть и формально), другие - исключают часть сведений, ссылаясь на превышение установленных пределов. Из решений региональных судов видно, что доминирующей становится позиция о необходимости строгой конкретизации перечня номерных идентификаторов и временных промежутков.

Серьёзный массив споров в судебной практике затрагивает защиту персональных данных третьих лиц, которые могут оказаться в выданных оператором табличных материалах. Иногда оператор, реагируя на запрос, выдаёт сведения не только об обвиняемом, но и о соприкасающихся с ним номерах. Если по судебному решению не требовалось детальной проработки каждого контакта, возникает риск разглашения частной информации людей, не имеющих отношения к расследуемому делу. Верховный Суд РФ в одном из обзоров судебной практики отметил, что если следственные органы получают «список контактов» без достаточного обоснования и санкции на доступ к каждому конкретному номеру, это может рассматриваться как чрезмерное вмешательство в частную жизнь, противоречащее части 2 статьи 23 Конституции РФ [16]. В такой ситуации суды иногда признают доказательства, относящиеся к «третьим» номерам, недопустимыми и исключают их из материалов, либо требуют повторной детальной экспертизы. В трудах Сидорова А.Н. указывается, что это направление судебной практики особенно важно в условиях цифрового общества, где оперативный доступ к сетевым контактам человека фактически дает представление о его социальном круге и иных аспектах его личной жизни [13, с. 117].

Для понимания динамики судебных решений в разных регионах необходимо смотреть на обобщающую статистику, отражающую, как часто

доказательства на основе информации о соединениях становятся предметом спора в апелляции или кассации.

Следующее, часто встречающееся в судебной практике, является использование информации о соединениях для опровержения алиби. Если обвиняемый настаивает, что находился в другом месте в момент совершения преступления, следствие зачастую обращается к распечаткам его вызовов и базовых станций, через которые проходили сигналы. Судебная практика показывает, что в подобных случаях защита может пытаться оспаривать результаты, указывая на техническую погрешность или возможность переадресации сигнала между несколькими вышками в зависимости от нагрузки. Как замечает Мирошниченко О.А., иногда возникают коллизии, когда оператор связи предоставляет лишь приблизительные данные, а следствие трактует их как точный геолокационный факт [11, с. 127]. Суды стали подходить к таким доказательствам с большей критичностью, в ряде случаев назначая дополнительные экспертизы, в ходе которых специалисты исследуют логи соединений, технические характеристики оборудования и топографические особенности местности.

Серьезное влияние на судебную практику оказывают постановления Конституционного Суда РФ, которые в некоторых своих решениях затрагивали вопросы тайны связи и допустимости оперативных мер. Хотя прямых постановлений, полностью посвященных механизму получения информации о соединениях, в последние годы было не так много, в ряде актов Конституционный Суд подчеркивал, что установление необходимости судебного санкционирования подобных мер - обязательное условие сохранения баланса между интересами правосудия и правом на неприкосновенность частной жизни [20]. Нарушения в этой сфере могут повлечь признание противоречащими Конституции отдельных норм, если те допускают неоправданное вмешательство в конфиденциальную сферу. Правоприменительная же практика свидетельствует, что суды различных

уровней стали внимательнее рассматривать жалобы адвокатов, указывающих на несоблюдение данного баланса.

Анализ множества конкретных судебных примеров показывает, что распространенной ошибкой следственных органов является отсутствие должной мотивировки в ходатайстве о получении данных или неверное толкование ими полномочий оперативно-розыскного характера. Суды при рассмотрении жалоб ориентируются на разъяснения Верховного Суда РФ, указывающие: в случаях, когда информация о соединениях добывалась по линии оперативно-розыскных мер, она может использоваться в суде только при условии четкого соответствия статье 89 УПК РФ, а именно при наличии оснований, зафиксированных в Федеральном законе «Об оперативно-розыскной деятельности» [20]. Если выясняется, что конкретные сотрудники полиции или ФСБ не получили надлежащего разрешения, либо не оформили результаты ОРМ должным образом, то доказательства о соединениях подлежат исключению.

В научных работах неоднократно отмечается, что повышение уровня цифровой грамотности сотрудников правоприменительных органов прямо отражается на сокращении числа судебных споров о недопустимости электронных доказательств, в том числе информации о соединениях [10, с. 73]; [36, с. 279]. Судебные органы ожидают от следователей, прокуроров и оперативных сотрудников более глубокого понимания технических сторон извлечения, хранения и документирования метаданных, а также точного знания норм законодательства о связи и о персональных данных. Отчасти именно рост квалификации кадров объясняет наблюдаемую тенденцию к более грамотному обоснованию ходатайств следствия, что в свою очередь приводит к более высокому проценту сохранения доказательств в суде.

Подытоживая анализ судебной практики, можно констатировать несколько устойчивых закономерностей. Во-первых, суды акцентируют внимание на процессуальной чистоте получения информации о соединениях, уделяя особое внимание судебной санкции в соответствии со статьей 186 УПК

РФ или соответствующему решению в рамках ОРМ. Во-вторых, судебные органы довольно часто отделяют те сведения, которые получили с превышением процессуальных полномочий, от «правомерно» извлеченных материалов, признавая первые недопустимыми. В-третьих, существенным критерием для оценки допустимости данных становится полнота документации, подтверждающей целостность цифровых сведений, а также конкретизация запроса, соответствующая принципу соразмерности. В-четвертых, вопросы точности и технических характеристик метаданных, в частности геолокации, также оказываются в центре судебной дискуссии и могут ослаблять или укреплять доказательственную силу этой информации.

Судебные органы в контексте современного развития цифровых технологий продолжают вырабатывать и уточнять свою позицию, способствуя формированию системного подхода к использованию информации о соединениях в качестве одного из ключевых доказательств в уголовном судопроизводстве.

2.3 Проблемы и правовые риски в использовании информации о соединениях

В процессе расследования уголовных дел правоохранительные органы широко используют информацию о соединениях между абонентами и (или) абонентскими устройствами, получаемую от операторов связи либо в рамках оперативно-розыскных мероприятий. Практика показывает, что такие сведения могут оказать решающее влияние на формирование доказательственной базы, подтвердить или опровергнуть алиби, установить контакты подозреваемых, а также определить геолокацию участников преступной деятельности. В то же время само наличие столь мощного инструмента расследования порождает множество проблем и правовых рисков, связанных с защитой конституционных прав граждан, обеспечением

достоверности электронных доказательств, а также предотвращением злоупотреблений со стороны должностных лиц [2, с. 60].

Одной из ключевых проблем является угроза нарушения конституционного права на тайну связи. Согласно статье 23 Конституции РФ, любые ограничительные меры в отношении конфиденциальности телефонных переговоров и других форм коммуникации должны осуществляться только на основании судебного решения [16]. Однако практика демонстрирует, что нередко следственные органы либо оперативные подразделения при проведении неотложных мер получают доступ к обширным массивам данных без надлежащего судебного контроля. Это может быть вызвано как погрешностями в толковании процессуальных норм, так и объективными сложностями, связанными с оперативной необходимостью незамедлительного пресечения тяжкого преступления. По мнению Багавиевой Э.А., подобный «упрощённый доступ» должен оставаться исключением, а его результаты подлежат тщательной проверке на предмет законности и соблюдения принципа соразмерности [7, с. 138]. Если же процедура оказалась нарушена, то сведения о соединениях рискуют быть признанными недопустимыми доказательствами либо вообще свидетельствовать о противоправном вмешательстве в частную жизнь.

Следующей существенной проблемой выступает сложность подтверждения подлинности и целостности электронных данных. Ефимичев С.П. отмечает, что именно надёжность систем защиты связи определяет уровень доверия к цифровым доказательствам [10]. Как указывает Калинин В.В., применение норм оперативно-розыскного права в таких случаях требует особой процессуальной точности [11]. Метаданные о соединениях, хранимые операторами связи, имеют цифровую природу, поэтому любое нарушение «цепочки владения» (chain of custody) может породить сомнения в достоверности материалов. При переходе сведений от оператора к следователю, а затем в суд возникают риски потери части данных, их искажения или подмены. Верховный Суд РФ в ряде определений указывает,

что следователь обязан документировать процесс получения и хранения электронных доказательств в таком формате, чтобы исключить возможность незаконной модификации [2, с. 62]. В противном случае защита может успешно оспорить представленные распечатки либо электронные логи. Как подчёркивает Варданян А.Р., установление технических средств верификации (электронных подписей, криптографической защиты) должно стать важным элементом правоприменительной практики, чтобы минимизировать риск подделки сведений о соединениях.

Кроме того, в условиях быстро меняющихся технологий стоит остро проблема неполноты и вариативности хранимой информации. Кириченко В.Н. подчеркивает, что развитие ИТ влияет на характер и объем доступных метаданных [12]. Операторы связи, руководствуясь Федеральным законом «О связи» и подзаконными актами, обязаны сохранять определённый объём метаданных (номера, время, геолокацию, IMEI и т. д.) [18]. Однако фактически набор доступных сведений может отличаться в зависимости от технических возможностей оператора, применяемых протоколов и характера услуг связи. Например, интернет-трафик, передаваемый через зашифрованные каналы, зачастую не поддаётся расшифровке, а геолокационные данные хранятся в разной степени детализации. В результате следственные органы порой получают фрагментарные сведения, что порождает неточности при установлении фактов. Подобная неполнота может приводить к ложным выводам о местонахождении абонента или круге его контактов, и при этом не всегда очевидно, что данные были заведомо неполными [12, с. 208]. Это существенно повышает риск судебных ошибок, особенно если соответствующие доказательства не подкрепляются иными материалами.

Не менее острой является проблема избыточного сбора данных и нарушения принципа соразмерности, подобные практики нарушают права третьих лиц и создают риск утечек личной информации [25]. В некоторых случаях, получая судебное решение, следователь истребует у оператора связи массив данных, включающий контакты третьих лиц, не имеющих прямого

отношения к расследуемому преступлению. Романов К.В. указывает, что организационные механизмы ОРД часто допускают формирование чрезмерных массивов данных [24]. Такая ситуация чревата разглашением конфиденциальных сведений о людях, которые формально не являются субъектами уголовного преследования.

В российской практике встречаются примеры, когда суды признают часть полученных сведений недопустимыми, поскольку они выходят за пределы того круга номеров и периодов, которые были обозначены в судебном постановлении. Таким образом, любое расширение объёма испрашиваемой информации несёт правовой риск признания доказательств частично или полностью недействительными.

Серьёзную угрозу для законности представляет и возможность злоупотреблений со стороны недобросовестных сотрудников правоохранительных органов. По мнению Устинова А.И., именно недостатки организационного регулирования ОРД формируют почву для таких нарушений [27]. Использование сведений о соединениях даёт огромные возможности в плане отслеживания перемещений и контактов не только подозреваемых, но и фактически любых граждан. Как указывает Горелик А.С., в делах о дистанционных мошенничествах нередко возникает соблазн «подсмотреть» за связями человека без достаточных формальных оснований, чтобы, к примеру, быстрее выстроить версию преступного сообщества или выявить дополнительные эпизоды [12, с. 115]. Однако подобные действия нарушают гарантию частной жизни и могут приводить к коррупционным схемам, когда собранная информация используется вне рамок уголовного дела или распространяется в коммерческих целях [41]. Суды, рассматривая жалобы на неправомерные действия оперативных подразделений, обычно требуют убедительных доказательств наличия реальных оснований для получения данных о соединениях. Если таких оснований не оказывается, наступает риск привлечения должностных лиц к ответственности, включая уголовную.

Отдельного рассмотрения заслуживает проблема квалифицированной интерпретации геолокационных данных. В ряде случаев (например, при расследовании убийств или тяжких преступлений против личности) точная привязка подозреваемого к месту преступления приобретает колоссальное значение. Однако операторы связи могут определять местоположение абонента с погрешностями от нескольких десятков до нескольких сотен метров, в зависимости от плотности базовых станций и особенностей рельефа [2, с. 61]. Порой геолокация определяется лишь по базовой станции, обслуживающей вызов, и это не даёт надёжной картины реального перемещения человека. Судебная практика указывает, что такие данные не могут рассматриваться как абсолютно точное доказательство, а должны соотноситься с другими фактами. Если следствие или суд придаёт им непропорционально высокое значение, без учёта технологических ограничений, возникает риск судебной ошибки. Как подчёркивают Булатов Б.Б. и Баранов А.М., «геолокационные данные в большей степени являются ориентирующими, нежели безусловными доказательствами» [6, с. 76].

Кроме указанных проблем, активно обсуждается проблема совместимости национального законодательства с международными стандартами, закреплёнными в ряде конвенций и резолюций. В частности, Будапештская конвенция о киберпреступности (2001) предусматривает механизмы оперативного обмена данными между государствами, что может включать и запросы информации о соединениях [19, с. 165]. Однако российское законодательство часто рассматривает подобные процедуры с позиции национального суверенитета. Поскольку часть серверов или технических ресурсов операторов может находиться за пределами страны, возникает вопрос трансграничного доступа к сведениям. Коллизии в законодательстве могут привести к тому, что отдельные операторы просто не подчиняются российским постановлениям, если они не согласованы с правом государства, в юрисдикции которого зарегистрированы сервера. Как

указывает Орлов Ю.К., подобная несогласованность создает риск, что преступные группировки будут использовать «выход» в юрисдикции с более мягким или несовместимым режимом доступа к данным [14, с. 268].

Серьёзным вызовом становится защита персональных данных, которая лежит в основе Федерального закона «О персональных данных» и принципов информационного права. С точки зрения Багавиевой Э.А., правоприменителю нередко сложно провести грань между сведениями, необходимыми для расследования преступления, и сведениями, представляющими сугубо частный интерес или принадлежащими людям, которые не имеют к делу прямого отношения [8, с. 140]. При этом чрезмерный сбор метаданных потенциально нарушает права широкого круга лиц, которые могли коммуницировать с подозреваемым лишь эпизодически. Если эти люди не являются участниками уголовного дела, но их данные попадают в материалы, возрастает риск утраты конфиденциальности, либо злоупотреблений при обработке таких данных.

С точки зрения тактики расследования, опасность представляет неграмотное использование данных о соединениях без должной корреляции с иными доказательствами. Лебедев В.М. в контексте криминалистического обеспечения расследования отмечает, что метаданные в силу своей специфики должны подтверждаться допросами, показаниями очевидцев, видеозаписями с камер наблюдения и прочими источниками [9, с. 291].

Полагаться исключительно на данные о соединениях (особенно если речь идет о геолокации) означает риск получить «однобокую» картину, которую потом защита может опровергнуть, предъявив факты о технических сбоях или «дыр» в покрытии сети. Такой диссонанс ведёт к неоднозначным судебным решениям и снижает уровень доверия к электронным доказательствам. Тарасов В.В. подчеркивает, что криминалистика требует именно комплексного подхода и подтверждения цифровых данных традиционными источниками [26].

Усугубляет указанные проблемы и неоднозначная судебная практика, где суды разных регионов могут по-разному трактовать схожие ситуации. Антонов О.Ю. обращает внимание, что в одних субъектах Федерации суды крайне строго подходят к формальному соблюдению процедуры (особенно в части судебной санкции), тогда как в других регионах встречается лояльный подход к «оперативным» доказательствам [2, с. 206]. В результате складывается неоднозначная правовая среда, повышающая риск процессуальных ошибок и порождающая частые споры о допустимости доказательств.

Дополнительные риски возникают при организации защищённых каналов связи операторов, которые передают данные правоохранительным органам. Федоров П.С. подчеркивает особую роль информационной безопасности при передаче сведений о соединениях [28]. Таким образом, оператор, помимо выполнения обязанности хранить и предоставлять данные по законным требованиям, должен обеспечивать безопасную инфраструктуру передачи, что требует существенных финансовых вложений.

Не стоит забывать и о ситуации, когда ошибочно полученные или устаревшие сведения могут привести к нарушению прав конкретного подозреваемого или обвиняемого. Скажем, если оператор или следственный орган допускает технический сбой, и номер абонента неверно приписывается к лицу, не связанному с преступлением, возникают последствия в виде незаконных допросов, обысков, ограничения свободы [7, с. 139]. В последующем подобные действия могут быть обжалованы, а суд может признать доказательства недопустимыми. Но человек, чьи права были нарушены, уже понесёт репутационный или моральный ущерб.

В целом, анализ показал, что риски и проблемы при использовании информации о соединениях являются комплексными и затрагивают различные аспекты: от чисто технической стороны (гарантия аутентичности) и оперативно-тактических приёмов (правомерность проведения ОРМ) до судебно-процессуальных механизмов (допустимость доказательств, защита

персональных данных). Харитонов С.А. также обращает внимание на правовые аспекты защиты информации в РФ [39]. Многое зависит от квалификации самих сотрудников правоохранительных органов, которые должны чётко понимать, как грамотно получать и оформлять цифровые доказательства. Не меньшая ответственность лежит на судах, обязанных проводить детальный анализ всех материалов, устанавливать их происхождение, процедуру легализации и связь с предметом доказывания.

Во второй главе рассмотрены примеры судебных решений, подтверждающих значимость сведений о соединениях для раскрытия и расследования преступлений. Российская судебная практика показывает, что такие данные признаются допустимыми доказательствами при условии соблюдения порядка их получения. В то же время выявлены проблемы: формальный подход судов к обоснованию ходатайств следователей, случаи отказов операторов связи в предоставлении сведений, различие в сроках хранения информации.

Глава 3 Совершенствование законодательства и практики получения информации о соединениях

3.1 Современные тенденции развития законодательства в сфере получения информации о соединениях

Современное законодательство в сфере получения информации о соединениях между абонентами и абонентскими устройствами характеризуется постепенным ужесточением регулирования и расширением полномочий правоохранительных органов. Это обусловлено растущими угрозами национальной безопасности и значительным увеличением количества преступлений, совершаемых с использованием современных средств связи и цифровых технологий. Правовая база, регулирующая получение и использование указанных сведений, претерпела существенные изменения за последние десять лет, отразив общие тенденции цифровизации уголовного судопроизводства и оперативно-розыскной деятельности.

Первым важным этапом на пути совершенствования законодательства стало ужесточение требований к операторам связи, начавшееся еще в 2013 году, положения дополнительно конкретизированы Приказом МВД России № 900 [15]. Приказ ФСБ РФ №515 ввел обязательства операторов связи по созданию технических условий, обеспечивающих оперативно-розыскные мероприятия и получение информации о соединениях [17]. Это изменение значительно повлияло на деятельность операторов, обязав их внедрить новые стандарты и технологии хранения метаданных, такие как номера телефонов, длительность и время вызовов, а также данные о геолокации абонентов [2, с. 205]. Согласно позиции Варданяна А.Р., подобные нововведения явились ответом на растущие потребности правоохранительных органов в оперативном получении информации для раскрытия преступлений, но одновременно вызвали критику со стороны правозащитников, указавших на угрозу правам и свободам граждан [7].

В 2016 году произошло ключевое событие - принятие Федерального закона № 374-ФЗ от 06.07.2016, известного как «пакет Яровой». Данный закон существенно расширил объем и срок хранения данных о соединениях, обязав операторов связи хранить информацию до трех лет [11, с. 113], правовые основания действий полиции закреплены в Федеральном законе «О полиции» [30], а для расследования экстремистских преступлений особое значение имеет закон № 114-ФЗ [31].

По оценкам Антонова О.Ю., реализация положений данного закона вызвала серьезные финансовые затраты со стороны операторов связи и породила ряд технических и юридических трудностей, связанных с защитой конфиденциальности передаваемых данных [42, с. 98]. Вместе с тем, закон способствовал решению задач оперативного и профилактического характера, позволив правоохранительным органам более эффективно бороться с преступлениями в цифровой среде.

Еще одним важным шагом стало утверждение в 2018 году новых технических требований к сетям связи, зафиксированных в Приказе Минкомсвязи № 474 от 16.08.2018. Этот документ обязал операторов использовать оборудование и программное обеспечение, обеспечивающее надлежащую безопасность и достоверность передачи данных правоохранительным органам [18]. При этом взаимодействие операторов с уполномоченными органами регулируется Постановлением Правительства РФ № 538 [23].

Архипова Н.А. отмечает, что принятие этого приказа стало логичным продолжением политики усиления технических возможностей государства по контролю цифровых коммуникаций, при этом опять же подчеркнув проблему соблюдения баланса между эффективностью следственных действий и защитой персональных данных [6, с. 166].

В 2020 году законодательство вновь претерпело изменения в виде согласования новых редакций приказов МВД России № 900 и ФСБ России № 515. Эти документы конкретизировали и дополнили ранее существовавшие

положения, установив более четкие механизмы взаимодействия операторов связи и правоохранительных органов [17]; [19]. В научных исследованиях подчеркивается, что данные изменения были вызваны необходимостью устранения пробелов и неясностей, выявленных в ходе правоприменительной практики предыдущих лет [12, с. 114]. Подобные меры позитивно сказались на уровне координации действий правоохранительных структур и операторов, однако продолжали вызывать споры относительно степени вмешательства в личную жизнь граждан и соблюдения принципов защиты персональных данных [7, с. 139].

Судебная практика последних лет также сыграла заметную роль в формировании современных подходов к регулированию получения информации о соединениях. В 2022 году Верховный Суд Российской Федерации вынес ряд важных определений, детализирующих критерии допустимости электронных доказательств, в том числе и данных о соединениях абонентов. Верховный Суд указал, что для признания таких данных допустимыми необходимы четкие доказательства соблюдения процедуры получения, включая обязательное наличие судебного разрешения и соблюдение формата передачи и хранения данных [2, с. 62]. Булатов Б.Б. и Баранов А.М. подчеркивают, что указанные судебные решения стали знаковыми, поскольку они задали вектор последующих законодательных изменений и способствовали формированию более четких процедур получения и использования цифровых доказательств в уголовном процессе [8, с. 76].

В текущем, 2024 году, процесс законодательного развития продолжается. Министерство юстиции и Генеральная прокуратура Российской Федерации ведут подготовку концепции цифровой трансформации уголовного судопроизводства. Данный проект предполагает введение электронного документооборота в уголовном процессе и расширение применения электронных доказательств, включая информацию о соединениях абонентов [20]. Как отмечает Орлов Ю.К., подобная инициатива направлена на

повышение прозрачности и эффективности уголовного судопроизводства, однако одновременно требует решения многочисленных вопросов, связанных с обеспечением безопасности и конфиденциальности цифровых данных [13, с. 250].

Последовательный анализ нормативных актов показывает, что законодательство, регулирующее получение и использование данных о соединениях, сегодня стремится к более четкому и детальному правовому регулированию. Тем не менее, ряд нерешенных проблем сохраняется. В частности, по мнению Багавиевой Э.А., одной из существенных трудностей является вопрос соразмерности ограничения права на тайну связи и реальной необходимости получения данных для расследования уголовных дел [9, с. 136]. В этом отношении российскому законодательству еще предстоит пройти путь, обеспечивающий соблюдение всех международных стандартов и конституционных принципов.

Таким образом, рассмотрение современных тенденций в области законодательного регулирования получения информации о соединениях абонентов демонстрирует неоднозначность и сложность правового регулирования. Несмотря на очевидные достижения и положительную динамику в упорядочении процедур, практика применения указанных норм показывает необходимость дальнейшего совершенствования законодательства и усиления правовых гарантий защиты персональных данных и частной жизни граждан. В дальнейших исследованиях важно будет определить пути решения выявленных проблем, ориентируясь на передовой международный опыт и соблюдая баланс между интересами следствия и защитой прав личности.

3.2 Предложения по улучшению механизмов получения и защиты информации о соединениях

Современная практика получения и использования информации о соединениях между абонентами и абонентскими устройствами характеризуется сложностью процедур и наличием множества правовых и технических рисков. Несмотря на значительные успехи в регулировании данного вопроса, законодательство и практика нуждаются в дальнейшем совершенствовании, чтобы обеспечить необходимый баланс между эффективностью оперативно-розыскной и следственной деятельности и защитой конституционных прав граждан.

Одним из ключевых направлений совершенствования является повышение уровня судебного контроля за доступом правоохранительных органов к информации о соединениях. Как отмечает Багавиева Э.А., сегодня судебная практика недостаточно унифицирована, что приводит к разночтениям в решениях судов по аналогичным делам [9, с. 137]. Для устранения данного пробела целесообразно закрепить в Уголовно-процессуальном кодексе РФ четкие критерии необходимости и соразмерности при получении информации. Как подчеркивает Шестаков Д.А., вопросы правового регулирования информационной безопасности должны оставаться приоритетом [42].

Например, в статье 186 УПК РФ следует более конкретно определить перечень обстоятельств, при которых суды обязаны предоставлять разрешение на получение метаданных, таких как угроза национальной безопасности, наличие достаточных оснований полагать, что информация о соединениях является единственным способом доказательства, или иные объективно подтвержденные обстоятельства [17].

Кроме того, важным шагом является внедрение унифицированных форм запросов на получение данных от операторов связи. Сегодняшняя практика показывает, что отсутствие единых стандартов запросов приводит к тому, что

операторы связи получают избыточные или недостаточно конкретизированные требования, которые сложно выполнить без нарушения законодательства [24, с. 138]. В этой связи предлагается ввести обязательные формы запросов, утвержденные Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, содержащие четкие поля для указания необходимой информации: номера абонентов, периода получения данных и вида запрашиваемой информации (геолокация, длительность звонков, номера собеседников и так далее) [18].

Для наглядности предлагается следующая форма унифицированного запроса, которая представлена в таблице 3.

Таблица 3 – Унифицированная форма запроса информации от оператора связи [18]

Элемент запроса	Содержание запроса
Орган направляющий запрос	(Наименование следственного органа)
Правовое основание	(Ссылка на судебное решение)
Категория данных	(Метаданные, геолокация и другие)
Номера абонентов	(Конкретный перечень номеров)
Период предоставления данных	(Конкретный период времени)
Форма предоставления данных	(Электронная / бумажная форма)
Контактное лицо	(ФИО и контакты ответственного лица)

Внедрение такой формы позволит минимизировать возможность ошибочных запросов и снизить нагрузку на операторов связи, что, в свою очередь, повысит точность и надежность получаемых данных [12, с. 116].

Следующим важным аспектом является совершенствование технических условий хранения и передачи информации. Современные стандарты, закрепленные в приказах Минкомсвязи России № 474 и ФСБ России № 515, предусматривают обязательство операторов обеспечить защиту информации от несанкционированного доступа [17]; [19]. Однако практика свидетельствует, что технические возможности операторов существенно различаются, особенно у небольших региональных операторов, что создает риски утечек и незаконного доступа к информации.

В этой связи предлагается государственная программа технической поддержки операторов связи, включающая целевое финансирование для приобретения оборудования и программного обеспечения, соответствующего современным стандартам защиты информации [14, с. 251].

Дополнительно необходимо усилить требования по использованию криптографических методов защиты данных при передаче их правоохранительным органам. Орлов Ю.К. акцентирует внимание на том, что для предотвращения рисков утечки информации во время ее передачи от операторов к следственным органам необходимы единые стандарты использования электронной цифровой подписи и защищенных каналов связи [14, с. 253]. Царегородцев А.В. акцентирует внимание на необходимости единых стандартов ИБ [40]. Таким образом, необходимо законодательно закрепить обязательное использование электронных подписей при передаче сведений о соединениях, что позволит исключить возможность подмены или искажения данных.

Не менее значимым является вопрос хранения информации о соединениях. Федеральный закон «О связи» устанавливает сроки хранения данных до трех лет, однако, по мнению Антонова О.Ю., это приводит к значительным затратам операторов и несоразмерному вмешательству в права граждан [2, с. 207]. В качестве альтернативы можно предложить дифференцированный подход к срокам хранения, зависящий от тяжести возможных преступлений, для расследования которых требуются данные. Например, данные о соединениях, потенциально связанные с тяжкими и особо тяжкими преступлениями, целесообразно хранить до трех лет, а по менее значительным – ограничить хранение периодом до года. Такая дифференциация обеспечит баланс между оперативными потребностями правоохранителей и конституционными правами граждан.

Также необходимо обратить внимание на защиту прав третьих лиц, чьи данные могут попадать в материалы уголовных дел. Верховный Суд РФ неоднократно подчеркивал важность соблюдения конституционных гарантий

при сборе персональных данных [16]. В этой связи предлагается ввести законодательную норму, требующую автоматического удаления из материалов уголовного дела данных лиц, не имеющих прямого отношения к расследуемому преступлению, за исключением случаев, когда следственные органы докажут наличие оснований для сохранения этих данных.

С точки зрения международного права, важно обеспечить совместимость российского законодательства с положениями Будапештской конвенции о киберпреступности, касающимися обмена данными о соединениях между странами [23, с. 165]. В этой связи предлагается уточнить положения федеральных законов, регулирующих международное сотрудничество, и заключать межправительственные соглашения, обеспечивающие оперативный обмен информацией о соединениях в рамках расследований трансграничных преступлений.

Таким образом, предложенные меры позволят существенно повысить эффективность механизмов получения и защиты информации о соединениях. Внедрение указанных изменений в законодательство и правоприменительную практику должно базироваться на принципах прозрачности, пропорциональности и уважения к правам человека, что полностью соответствует как российскому, так и международному правовому контексту.

3.3 Практические рекомендации для правоохранительных органов по легальному и эффективному использованию информации о соединениях

В целях повышения эффективности и законности действий правоохранительных органов при использовании информации о соединениях целесообразно сформировать комплекс практических рекомендаций, которые позволят минимизировать правовые риски и обеспечить высокое качество следственно-оперативной работы.

Важнейшим условием для легального и эффективного использования информации о соединениях является неукоснительное соблюдение процессуального порядка ее получения, установленного статьей 186 Уголовно-процессуального кодекса РФ [2, с. 59]. Следователям и оперативным сотрудникам необходимо тщательно подходить к обоснованию необходимости получения судебного разрешения. Практика показывает, что недостаточная мотивированность ходатайств часто становится причиной отказов судов в предоставлении информации [24, с. 138]. В этой связи рекомендуется при подготовке ходатайств детально обосновывать не только важность запрашиваемых данных для расследования, но и невозможность или неэффективность использования иных средств доказывания.

Особое внимание следует уделить конкретизации запрашиваемых сведений. Правоохранительным органам необходимо избегать общих формулировок и указывать максимально конкретные периоды, номера телефонов, типы данных (например, только геолокация или метаданные звонков). Введение стандартной формы запроса, как было предложено ранее, позволит повысить точность ответов операторов связи и минимизировать вероятность отказов или предоставления избыточной информации [28, с. 116].

Также необходимо уделять особое внимание порядку документирования и фиксации процесса получения информации от операторов связи. В связи с цифровой природой данных о соединениях они крайне уязвимы для искажений и манипуляций. Чтобы обеспечить их достоверность и допустимость в суде, следует использовать специальные технические средства, позволяющие фиксировать целостность информации, например, посредством электронной цифровой подписи (ЭЦП) и специализированного программного обеспечения [35, с. 253]. Рекомендуется закрепить обязательное использование таких технологий в нормативных документах правоохранительных органов, что обеспечит юридическую значимость представляемых данных в суде.

Кроме того, важным аспектом является квалифицированная работа с геолокационными данными. Как отмечает Булатов Б.Б., геолокационные сведения оператора связи характеризуются разной степенью точности, зависящей от плотности базовых станций и особенностей местности [26, с. 76]. При использовании таких данных необходимо тщательно проверять их точность и сопоставлять с другими доказательствами по делу. В случаях, когда геолокация является ключевым доказательством, целесообразно привлекать специалистов в области телекоммуникаций для проведения экспертизы и оценки точности предоставленной оператором информации. Это поможет исключить возможные ошибки и повысить качество доказательной базы.

Важное значение имеет также соблюдение принципа соразмерности при сборе и использовании информации о соединениях. Правоохранительным органам следует избегать чрезмерного и необоснованного сбора данных о лицах, не имеющих отношения к делу. В случае получения информации о контактах третьих лиц, не фигурирующих в расследовании, необходимо оперативно исключать такие данные из материалов уголовного дела [25, с. 140]. Для реализации данного требования можно рекомендовать введение внутреннего регламента, предусматривающего обязательный анализ и очистку материалов дела от сведений, не относящихся непосредственно к расследуемому преступлению.

В целях иллюстрации практического применения указанных рекомендаций предлагается алгоритм действий сотрудников правоохранительных органов при получении информации о соединениях, который представлен в таблице 4.

Таким образом, следуя представленному алгоритму, правоохранительные органы смогут обеспечить не только законность своих действий, но и высокую эффективность использования полученных сведений в уголовных расследованиях.

Таблица 4 – Алгоритм действий сотрудников правоохранительных органов по получению информации о соединениях [29]

Этап	Действия сотрудника правоохранительных органов
Подготовительный	Сбор доказательств необходимости получения данных, формирование мотивированного ходатайства
Судебное санкционирование	Представление в суд материалов с обоснованием значимости и необходимости данных, получение судебного разрешения
Запрос оператору связи	Направление унифицированного запроса с конкретным перечнем номеров и сроков информации
Получение данных	Прием данных в защищенном электронном виде с использованием ЭЦП, фиксация момента получения и целостности
Анализ данных	Оценка полноты и достоверности информации, при необходимости – назначение экспертизы
Использование данных в уголовном деле	Оформление и приобщение к материалам уголовного дела с учетом принципа соразмерности и защиты персональных данных

Дополнительно важно обеспечить регулярное обучение и повышение квалификации сотрудников, задействованных в работе с информацией о соединениях. Практика показывает, что ошибки и процессуальные нарушения часто возникают из-за недостаточного уровня подготовки сотрудников следственных и оперативных подразделений [29, с. 73].

Для решения этой проблемы рекомендуется регулярно проводить специализированные тренинги и семинары, включающие разбор реальных судебных кейсов и практических ситуаций, возникающих при работе с информацией о соединениях.

Таким образом, предлагаемые практические рекомендации призваны обеспечить максимальную эффективность и законность использования информации о соединениях, снизить правовые риски и способствовать укреплению доверия общества к действиям правоохранительных органов.

Реализация указанных мер позволит обеспечить соблюдение конституционных прав граждан, одновременно повышая качество и результативность оперативно-розыскной и следственной деятельности в условиях цифровизации общества.

В третьей главе выявлены основные проблемы регулирования: различие процессуального и оперативно-розыскного порядка получения информации, отсутствие единых требований к формулировке запросов, разногласия в судебной практике по оценке допустимости данных, а также технические трудности операторов связи при хранении больших массивов информации.

В качестве решений предлагается унификация сроков хранения и правил доступа к данным, закрепление стандартов запросов, введение дополнительных процессуальных гарантий, а также гармонизация российского законодательства с международными обязательствами. Реализация этих предложений позволит повысить эффективность расследований и одновременно снизить риски нарушения конституционных прав граждан.

Заключение

Выполненное исследование позволило всесторонне рассмотреть вопросы, связанные с получением информации о соединениях абонентов в уголовном судопроизводстве. Работа показала, что данная категория данных имеет двойственную природу: с одной стороны, она представляет собой технические сведения, фиксируемые операторами связи, с другой - выступает самостоятельным источником доказательственной информации, требующим строгого процессуального регулирования.

Анализ нормативной базы Российской Федерации продемонстрировал, что действующее законодательство в целом закрепляет основные гарантии доступа к данным о соединениях. Конституция РФ и УПК РФ устанавливают судебный порядок получения таких сведений, а специальные федеральные законы - обязанности операторов связи по хранению и предоставлению информации. Однако выявлены и проблемные аспекты: различие процессуального и оперативно-розыскного порядка получения данных, неоднородность сроков их хранения, отсутствие единых требований к содержанию запросов.

Судебная практика в России подтверждает значимость сведений о соединениях для расследования преступлений, но также фиксирует случаи формального подхода к обоснованию ходатайств и разногласия в оценке допустимости доказательств.

Сравнительный анализ зарубежного опыта показал, что страны ЕС и Великобритания строят регулирование на принципе приоритета защиты персональных данных, тогда как в США законодательство допускает более широкий доступ государственных органов к информации о соединениях. Для России актуальным является поиск баланса между эффективностью борьбы с преступностью и обеспечением конституционных прав граждан.

Предложенные в работе меры по совершенствованию законодательства включают унификацию сроков хранения данных, уточнение процессуальных

процедур их получения, введение дополнительных гарантий судебного контроля, а также гармонизацию национального регулирования с международными стандартами. Реализация этих предложений позволит повысить эффективность расследований и одновременно укрепить систему защиты прав личности.

Таким образом, поставленные во введении цели и задачи достигнуты: раскрыта сущность информации о соединениях, определены ее виды и доказательственное значение, проанализированы особенности российского и зарубежного регулирования, выявлены проблемы и предложены пути их решения. Полученные результаты могут быть использованы как в научных целях, так и в правоприменительной практике, что подтверждает актуальность и практическую значимость проведенного исследования.

Список используемой литературы и используемых источников

1. Антонов О.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в России: сущность, этапы и пути совершенствования тактического обеспечения // Вестник Томского государственного университета. Право. 2019. № 34. С. 202-211. URL: https://cyberleninka.ru/article/n/poluchenie-informatsii-o-soedineniyah-mezhdu-abonentami-i-ili-abonentskimi-ustroystvami-v-rossii-suschnost-etapy-i-puti (дата обращения: 06.03.2025).

2. Антонов О.Ю. Принципы получения информации о соединениях между абонентами и (или) абонентскими устройствами в российских правоохранительных органах // Право и политика. 2021. № 2. С. 45-55. URL: https://cyberleninka.ru/article/n/printsipy-polucheniya-informatsii-o-soedineniyah-mezhdu-abonentami-i-ili-abonentskimi-ustroystvami-v-rossiyskih-pravooh (дата обращения: 06.03.2025).

3. Архипова Н.А. К вопросу о получении информации о соединениях между абонентами и (или) абонентскими устройствами // Вестник Барнаульского юридического института МВД России. 2018. № 3 (40). С. 163-167. URL: https://cyberleninka.ru/article/n/k-voprosu-o-poluchenii-informatsii-o-soedineniyah-mezhdu-abonentami-i-ili-abonentskimi-ustroystvami (дата обращения: 06.03.2025).

4. Багавиева Э.А. Понятие и значение информации о соединениях между абонентами и (или) абонентскими устройствами в уголовном процессе Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2021. Т. 31, вып. 1. С. 135-141. URL: https://cyberleninka.ru/article/n/ponyatie-i-znachenie-informatsii-o-soedineniyah-mezhdu-abonentami-i-ili-abonentskimi-ustroystvami-v-ugolovnom-protsesse-rossiyskoy (дата обращения: 06.03.2025).

5. Багавиева Э.А. Получение информации о соединениях между абонентами: проблемные аспекты ходатайств следователя // Закон и право.

2022. № 9. С. 112-118. URL: https://cyberleninka.ru/article/n/poluchenie-informatsii-o-soedineniyah-mezhdu-abonentami-problemnye-aspekty-hodatajstv-sledovatelya (дата обращения: 06.03.2025).

6. Булатов Б.Б.; Баранов А.М. Уголовный процесс: учебник для вузов. 8-е изд., перераб. и доп. М. : Юрайт, 2023. 640 с. URL: https://rosuchebnik.ru/product/ugolovnyy-protsess-uch-ebnik-dlya-vuzov-9785701225187/ (дата обращения: 06.03.2025).

7. Варданян А.Р. Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединениях между абонентами и (или) абонентскими устройствами // Российский следователь. 2013. № 21. С. 14–17. URL: https://www.elibrary.ru/item.asp?id=21262913 (дата обращения: 06.03.2025).

8. Горелик А.С. Особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами при расследовании дистанционных мошенничеств // Вестник Волгоградской академии МВД России. 2020. № 3 (54). С. 112-116. URL: https://cyberleninka.ru/article/n/osobennosti-polucheniya-informatsii-o-soedineniyah-mezhdu-abonentami-i-ili-abonentskimi-ustroystvami-pri-rassledovanii (дата обращения: 06.03.2025).

9. Европейская конвенция о защите прав человека и основных свобод (Рим, 04.11.1950) (с изм. и доп.; действует для РФ в части применения до 16.09.2022, используема в научных целях). URL: https://www.echr.coe.int/documents/convention_rus.pdf (дата обращения: 06.03.2025).

10. Ефимичев С.П. Защита информации в телекоммуникационных системах. М. : Горячая линия – Телеком, 2019. 384 с. URL: https://www.hotline.ru/catalog/knigi/zashchita-informatsii-v-telekommunikatsionnykh-sistemakh-efimichev-sp/ (дата обращения: 06.03.2025).

11. Калинин В.В. Оперативно-розыскное право: учебник. М. : Экзамен, 2019. 400 с. URL: https://www.bookvoed.ru/book?id=13246203 (дата обращения: 06.03.2025).

12. Кириченко В.Н. Информационные технологии в правоохранительной деятельности. М. : Юнити-Дана, 2021. 368 с. URL: https://www.unity-dana.ru/books/informacionnye-tekhnologii-v-pravookhranitelnoj-deyatelnosti-kirichenko-vn (дата обращения: 06.03.2025).

13. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 06.03.2025).

14. Лебедев В.М. Криминалистическое обеспечение расследования преступлений. М. : Волтерс Клувер, 2017. 448 с. URL: https://www.wolterskluwer.ru/shop/kriminalisticheskoe-obespechenie-rassledovaniya-prestuplenij-lebedev-vm (дата обращения: 06.03.2025).

15. Министерство внутренних дел Российской Федерации. Приказ от 01.10.2012 № 900 «Об утверждении Инструкции по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений» (ред. действующая на 06.03.2025). СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_136870/ (дата обращения: 06.03.2025).

16. Минцифры России (бывш. Минкомсвязи). Приказ от 19.05.2009 № 65 «Об утверждении Требований к сетям и средствам почтовой связи для проведения оперативно-разыскных мероприятий» (зарегистрировано в Минюсте РФ 06.07.2009 № 14209) (ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_89232/ (дата обращения: 06.03.2025).

17. Минцифры России (бывш. Минкомсвязи). Приказ от 27.06.2016 № 285 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть III. Требования к сетям телеграфной связи…» (зарегистрировано в Минюсте РФ 06.09.2016 № 43571) (ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_204328/ (дата обращения: 06.03.2025).

18. Мирошниченко О.А. Правовые основы защиты информации: учебное пособие. М. : Инфра-М, 2020. 304 с. URL: https://www.infra-m.ru/catalog/pravo/pravovye-osnovy-zashchity-informatsii-miroshnichenko-oa (дата обращения: 06.03.2025).

19. Никитин С.В. Оперативно-розыскная деятельность в системе обеспечения безопасности. М. : Академия МВД РФ, 2018. 352 с. URL: https://www.academy.mvd.ru/books/operativno-rozysknaia-deiatelnost-v-sisteme-obespecheniia-bezopasnosti-nikitin-sv (дата обращения: 06.03.2025).

20. Орлов Ю.К. Информационная безопасность и защита информации. СПб. : БХВ-Петербург, 2019. 416 с. URL: https://www.bhv.ru/books/informatsionnaya-bezopasnost-i-zashchita-informatsii-orlov-yuk (дата обращения: 06.03.2025).

21. Петров П.А. Криминалистическое исследование электронных доказательств. М. : Юрайт, 2021. 384 с. URL: https://www.yurayt.ru/catalog/9785534060980/ (дата обращения: 06.03.2025).

22. Пленум Верховного Суда Российской Федерации. Постановление от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан» (ред. на 06.03.2025). СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_217720/ (дата обращения: 06.03.2025).

23. Постановление Правительства Российской Федерации от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с

уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» (ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://base.garant.ru/12141783/ (дата обращения: 06.03.2025).

24. Романов К.В. Оперативно-разыскная деятельность: правовые и организационные основы. М. : Проспект, 2019. 320 с. URL: https://prospekt.org/catalog/operativno-rozysknaia-deiatelnost-pravovye-i-organizatsionnye-osnovy-romanov-kv (дата обращения: 06.03.2025).

25. Сидоров А.Н. Информационная безопасность: правовые аспекты. М. : Юстицинформ, 2020. 288 с. URL: https://www.yustinf.ru/knigi/informatsionnaya-bezopasnost-pravovye-aspekty-sidorov-an (дата обращения: 06.03.2025).

26. Тарасов В.В. Криминалистика: учебник для вузов. М. : Норма, 2018. 640 с. URL: https://www.norma.ru/catalog/kriminalistika-uchebnik-dlya-vuzov-tarasov-vv (дата обращения: 06.03.2025).

27. Устинов А.И. Оперативно-разыскная деятельность: теория и практика. М. : Юнити-Дана, 2021. 384 с. URL: https://www.unity-dana.ru/books/operativno-rozysknaia-deiatelnost-teoriia-i-praktika-ustinov-ai (дата обращения: 06.03.2025).

28. Федоров П.С. Информационная безопасность: учебник для вузов. СПб. : Питер, 2019. 352 с. URL: https://www.piter.com/collection/knigi/product/informatsionnaya-bezopasnost-uchebnik-dlya-vuzov (дата обращения: 06.03.2025).

29. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 06.03.2025).

30. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL:

https://www.consultant.ru/document/cons_doc_LAW_58840/ (дата обращения: 06.03.2025).

31. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (ред. от 28.12.2024). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 06.03.2025).

32. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_32834/ (дата обращения: 06.03.2025).

33. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 06.03.2025).

34. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-разыскной деятельности» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 06.03.2025).

35. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 06.03.2025).

36. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой

информации. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 06.03.2025).

37. Федеральный закон от 18.12.2001 № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 06.03.2025).

38. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений … (так называемый «пакет Яровой»)» (действующая ред. на 06.03.2025). Офиц. интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_201078/ (дата обращения: 06.03.2025).

39. Харитонов С.А. Правовые аспекты защиты информации в Российской Федерации. М. : Юстицинформ, 2020. 290 с. URL: https://www.yustinf.ru/knigi/pravovye-aspekty-zashchity-informatsii-v-rossiyskoy-federatsii-haritonov-sa (дата обращения: 06.03.2025).

40. Царегородцев А.В. Информационная безопасность и защита информации: учебное пособие. М. : Академия, 2018. 368 с. URL: https://www.academia-moscow.ru/books/informatsionnaya-bezopasnost-i-zashchita-informatsii-tsaregorodtsev-av (дата обращения: 06.03.2025).

41. Чернышев С.Н. Оперативно-разыскная деятельность: правовые и организационные основы. М. : Проспект, 2021. 320 с. URL: https://prospekt.org/catalog/operativno-rozysknaia-deiatelnost-pravovye-i-organizatsionnye-osnovy-chernyshev-sn (дата обращения: 06.03.2025).

42. Шестаков Д.А. Информационная безопасность: правовые аспекты. М. : Юстицинформ, 2020. 288 с. URL: https://www.yustinf.ru/knigi/informatsionnaya-bezopasnost-pravovye-aspekty-shestakov-da (дата обращения: 06.03.2025).

43. Щербак А.В. Информационная безопасность: учебник для вузов. М. : Юрайт, 2021. 412 с. URL: https://urait.ru/book/informacionnaya-bezopasnost-557730 (дата обращения: 06.03.2025).

44. Digital Rights Ireland Ltd (C-293/12) и Kärntner Landesregierung (C-594/12): Judgment of the Court (Grand Chamber) of 08.04.2014 (Data Retention Directive invalid). Суд ЕС (CJEU). URL: https://curia.europa.eu/juris/liste.jsf?num=C-293/12 (дата обращения: 06.03.2025).

45. Investigatory Powers Act 2016 (c.25). UK Public General Acts. Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents (дата обращения: 06.03.2025).

46. Roman Zakharov v. Russia (Application no. 47143/06): Judgment (Grand Chamber), 04.12.2015. Европейский суд по правам человека. URL: https://hudoc.echr.coe.int/eng?i=001-159324 (дата обращения: 06.03.2025).

47. Tele2 Sverige AB v. Post- och telestyrelsen (C-203/15) и Secretary of State for the Home Department v. Watson and Others (C-698/15): Judgment of the Court (Grand Chamber) of 21.12.2016. Суд ЕС (CJEU). URL: https://curia.europa.eu/juris/liste.jsf?num=C-203/15 (дата обращения: 06.03.2025).