

Дата поступления рукописи в редакцию: 05.09.2026 г.

DOI: 10.24412/2782-3849-2026-10-58-62

Дата принятия рукописи в печать: 26.10.2026 г.

**ВОЛЧЕНКО Анастасия Владимировна,**

кандидат юридических наук, старший преподаватель кафедры  
уголовного процесса Белгородского юридического института  
МВД России имени И.Д. Путилина,  
e-mail: espy207@yandex.ru

**ШЕЛЯКИН Алексей Васильевич,**

старший преподаватель кафедры гражданско-правовых  
дисциплин факультета подготовки следователей ФГКОУВО  
«Московская академия Следственного комитета Российской  
Федерации имени А.Я. Сухарева»,  
e-mail: aleksei9492@mail.ru

### **ТАЙНА ПЕРЕПИСКИ В МЕССЕНДЖЕРАХ В ЦИФРОВОЙ СРЕДЕ: ПРОЦЕССУАЛЬНЫЕ ГАРАНТИИ ОТ ПРОИЗВОЛЬНОГО ДОСТУПА ГОСУДАРСТВА**

**Аннотация.** Исследование посвящено процессуальным гарантиям обеспечения тайны переписки, осуществляемой посредством мессенджеров, в уголовном судопроизводстве Российской Федерации. Установлена нормативно-процессуальная асимметрия, выражающаяся в том, что получение сведений о коммуникациях у операторов связи допускается на основании судебного решения, тогда как доступ к содержимому памяти правомерно изъятого мобильного устройства, исходя из правовой позиции Конституционного Суда Российской Федерации, не предполагает обязательного получения самостоятельной судебной санкции. Обоснован принцип функциональной эквивалентности процессуального вмешательства, согласно которому объем гарантий должен определяться характером, содержанием и интенсивностью доступа к частной коммуникации, а не техническим способом хранения соответствующей информации. Предложена модель судебно-санкционируемого доступа к цифровой переписке, предусматривающая предметную и временную конкретизацию объема исследования, минимизацию избыточного вмешательства, обязательную техническую фиксацию процессуальных действий и специальный порядок осуществления доступа в условиях неотложности.

**Ключевые слова:** неприкосновенность частной жизни, тайна переписки, мессенджеры, цифровые доказательства, судебный контроль, уголовный процесс, допустимость доказательств.

**VOLCHENKO Anastasia Vladimirovna,**

Ph.D., Senior Lecturer, Department of Criminal Procedure, Belgorod  
Law Institute of the Ministry of Internal Affairs of Russia named  
after I.D. Putilin

**SHELYAKIN Alexey Vasilievich,**

Senior Lecturer, Department of Civil Law Disciplines, Faculty of  
Training of Investigators, FGKOUVO "Moscow Academy of the  
Investigative Committee of the Russian Federation named after  
A. Ya. Sukharev"

### **SECRECY OF CORRESPONDENCE IN MESSENGERS IN THE DIGITAL ENVIRONMENT: PROCEDURAL GUARANTEES AGAINST ARBITRARY ACCESS OF THE STATE**

**Annotation.** The study is devoted to the procedural guarantees of ensuring the secrecy of correspondence carried out through messengers in the criminal proceedings of the Russian Federation. A regulatory and procedural asymmetry has been established, which is expressed in the fact that obtaining information about communications from telecom operators is allowed on the basis of a court decision, whereas access to the contents of the memory of a lawfully seized mobile device, based on the legal position of the Constitutional Court of the Russian Federation, does not necessarily imply obtaining an independent judicial sanction. The principle of functional equivalence

of procedural intervention is substantiated, according to which the scope of guarantees should be determined by the nature, content and intensity of access to private communication, rather than by the technical method of storing relevant information. A model of judicially sanctioned access to digital correspondence is proposed, which provides for substantive and temporary specification of the scope of research, minimization of excessive interference, mandatory technical fixation of procedural actions and a special procedure for access in urgent conditions.

**Key words:** right to privacy, confidentiality of correspondence, instant messaging apps, digital evidence, judicial oversight, criminal proceedings, admissibility of evidence.

#### Введение

Развитие цифровых форм коммуникации обусловило существенное усложнение содержания конституционно охраняемой сферы частной жизни. Современные мессенджеры обеспечивают хранение не только текстовых сообщений, но и медиавложений, сведений о контактах, времени и характере взаимодействия между пользователями, а также иной информации, позволяющей реконструировать значительный объем частной коммуникации. В связи с этим доступ к соответствующему приложению объективно влечет ознакомление не с единичным сообщением, а с совокупностью сведений, относящихся к частной жизни лица. Конституция Российской Федерации (ч. 2 ст. 23) и ст. 13 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) гарантируют тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, устанавливая, что ограничение данного права допускается исключительно на основании судебного решения.

Вместе с тем, уголовно-процессуальное законодательство дифференцирует объем гарантий в зависимости от технического способа получения информации. Контроль переговоров и получение сведений о соединениях осуществляются на основании судебного решения, тогда как специальный процессуальный порядок целевого доступа к ранее состоявшейся переписке, содержащейся в памяти изъятого электронного устройства, УПК РФ не предусматривает. Согласно правовой позиции Конституционного Суда Российской Федерации, осмотр и экспертное исследование информации, содержащейся в памяти законно изъятого устройства, не требуют самостоятельного судебного разрешения; соответствующий подход применяется и к доступу к переписке, осуществляемой посредством WhatsApp [1; 2].

В результате сведения, обладающие единым конституционно-правовым содержанием, получают различный уровень предварительной процессуальной защиты в зависимости от способа и источника их извлечения. Само по себе уведомление владельца об изъятии устройства, равно как и возможность последующего обжалования действий должностных лиц в порядке ст. 125 УПК РФ, не исключают ознакомления с сообщениями, не имеющими отношения к предмету

расследования. После фактического раскрытия таких сведений восстановление их конфиденциальности становится невозможным. В связи с этим, в современной уголовно-процессуальной доктрине обосновываются презумпция конфиденциальности цифровой информации, необходимость разграничения электронно-технических действий с учетом интенсивности вмешательства в частную сферу и усиление предварительного судебного контроля [4, с. 80-81; 5, с. 191; 7, с. 134; 9, с. 102].

Уголовно-правовая охрана тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений обеспечивается ст. 138 УК РФ и распространяется в том числе на коммуникацию, осуществляемую посредством цифровых сервисов. Масштаб применения процессуальных и оперативно-розыскных мер, сопряженных с ограничением конфиденциальности коммуникаций, подтверждается официальной судебной статистикой. Так, за первое полугодие 2025 г. в суды Российской Федерации поступило около 1,3 млн процессуальных обращений правоохранительных органов, из которых около 247 тыс. были связаны с ограничением конституционного права на тайну переписки и телефонных переговоров. В указанном периоде поступило 7,3 тыс. ходатайств о контроле и записи телефонных и иных переговоров и около 96 тыс. ходатайств о получении информации о соединениях между абонентами и (или) абонентскими устройствам [8]. При этом случаи исследования переписки, содержащейся на изъятых электронных устройствах, самостоятельному статистическому учету не подлежат. В связи с этим целью исследования является определение процессуального стандарта доступа к содержанию мессенджеров, обеспечивающего защиту частной коммуникации от необоснованного и избыточного вмешательства государства.

#### Основная часть

Принципиальное значение имеет разграничение правомерного физического обладания электронным устройством и процессуального доступа к содержащейся в его памяти информации. Законное изъятие смартфона обеспечивает сохранность соответствующего объекта, возможность его идентификации и последующего исследования, однако само по себе не устраняет режим

конфиденциальности содержащихся в нем сведений. Современное мобильное устройство аккумулирует значительный массив информации, относящейся к различным видам охраняемой законом тайны. Поэтому объем процессуальных гарантий должен определяться характером исследуемых данных и интенсивностью вмешательства в частную жизнь лица.

На этой основе представляется возможным сформулировать принцип функциональной эквивалентности процессуального вмешательства, согласно которому сопоставимый по содержанию и интенсивности доступ к частной коммуникации должен обеспечиваться равноценными процессуальными гарантиями независимо от технического способа получения соответствующих сведений. Перехват сообщения в процессе его передачи, получение его содержания от третьего лица и ознакомление с тем же сообщением, сохраненным в архиве мессенджера, различаются способом извлечения информации, однако затрагивают один и тот же конституционно охраняемый интерес – конфиденциальность частной коммуникации. Указанный подход развивает сформулированную в научной литературе презумпцию конфиденциальности информации, содержащейся в электронной памяти устройства, и предполагает возложение на сторону обвинения обязанности обосновать правомерность соответствующего вмешательства [7, с. 134].

Реализация принципа функциональной эквивалентности требует разграничения технических действий с электронным устройством и непосредственного доступа к содержанию частной коммуникации. Не каждое действие со смартфоном предполагает необходимость самостоятельного судебного разрешения. Фиксация внешнего состояния устройства и его идентификаторов, упаковка, изоляция от сети, а также создание криминалистической копии без ознакомления с содержащейся информацией могут осуществляться в рамках его изъятия и первоначального исследования. Иной процессуальный характер приобретает открытие мессенджера, поиск по переписке, просмотр вложений, восстановление удаленных сообщений либо использование сохраненной авторизации для получения облачных данных, поскольку в таких случаях непосредственным объектом исследования становится частная электронная коммуникация.

Предварительный судебный контроль доступа к частной коммуникации должен охватывать наличие конкретных данных о доказательственном значении переписки и ее связи с расследуемым событием, соразмерность вмешательства процессуальной цели и возможность получения необходимых сведений способом, в меньшей степени затрагивающим частную жизнь.

В судебном решении подлежат индивидуализации мессенджер или учетная запись, временной интервал, исследуемые диалоги либо категории сообщений, а при необходимости – облачные данные. Разрешение на осмотр устройства с общей формулой об извлечении сведений, «имеющих значение для уголовного дела», не определяет объем цифрового исследования и не исключает избыточного проникновения в жизнь человека.

Конкретизация судебного разрешения должна сочетаться с минимизацией вмешательства и технической проверяемостью исследования. Доступ к заведомо не относящимся к делу чатам и сообщениям недопустим; по достижении процессуальной цели дальнейшее исследование содержимого устройства прекращается. При создании полной криминалистической копии ее целесообразно хранить обособленно от материалов, непосредственно исследуемых по делу. В протоколе либо специальном электронном журнале должны фиксироваться идентификаторы устройства, способ доступа, его сетевое состояние, примененное программное обеспечение, факт создания копии и ее хэш-значение, последовательность поисковых действий, исследованный временной интервал, а также обращение к удаленным или облачным данным. Такая фиксация обеспечивает последующую проверку целостности цифровой информации и правомерности произведенного вмешательства.

Отступление от предварительного судебного контроля может быть оправдано только наличием конкретной и реально существующей угрозы утраты цифровых данных. В подобных случаях следователь вправе незамедлительно принять меры по их сохранению, а при объективной невозможности обеспечить сохранность без ознакомления с содержанием – осуществить доступ исключительно в объеме, необходимом для предотвращения утраты информации, с последующей судебной проверкой законности и обоснованности произведенных действий. Самостоятельного регулирования требует и добровольное согласие владельца устройства. Таковое может исключать необходимость предварительного судебного разрешения лишь при условии его свободного, информированного и конкретного характера с указанием соответствующего приложения, временного интервала либо определенного диалога. Передача устройства или сообщения кода разблокирования не может рассматриваться как безусловный отказ от конфиденциальности всей содержащейся в нем переписки.

Указанный подход соотносится с предложениями, сформулированными в современной уголовно-процессуальной доктрине, о введении специального порядка исследования мобильных устройств, презумпции конфиденциальности

цифровых данных и дифференциации процессуальных действий с учетом интенсивности вмешательства [6, с. 127; 7, с. 134; 9, с. 102, 105-106]. Вместе с тем, привязка специального регулирования исключительно к «осмотру телефона» представляется технологически ограниченной. Объектом процессуальной охраны должны признаваться сведения, составляющие содержание частной электронной коммуникации, независимо от конкретного технического средства доступа к ним – смартфона, компьютера, планшета, веб-клиента либо иного цифрового интерфейса [3; 4, с. 80-81].

Последовательная реализация изложенного подхода требует его закрепления непосредственно в уголовно-процессуальном законе. Такую модель целесообразно закрепить путем дополнения ст. 13 и ч.2 ст.29 УПК РФ, а также введения ст. 186.2 УПК РФ «Получение и исследование сведений частных электронных коммуникаций». Целевой доступ к электронным сообщениям, содержащимся в памяти устройства либо доступным через учетную запись или информационную систему, должен осуществляться по судебному решению. Исключения допустимы лишь при конкретном добровольном согласии лица либо в прямо предусмотренных законом неотложных случаях.

Ходатайство следователя и судебное постановление должны содержать фактические основания доступа, данные о лице, устройстве или учетной записи, вид и временной интервал исследуемой информации, ее связь с обстоятельствами, подлежащими доказыванию, способ извлечения, возможность удаленного доступа, меры минимизации и порядок технической фиксации. Выход за разрешенный объем при отсутствии неотложности требует нового судебного решения. Существенное нарушение установленного порядка подлежит оценке по правилам ст. 75 УПК РФ. После отпадения оснований для сохранения конфиденциальности, лицу следует сообщить фактический объем доступа, обеспечив возможность обжалования в порядке ст. 125 УПК РФ.

Предлагаемая модель согласуется с правовыми позициями Конституционного Суда Российской Федерации, выраженными в определениях от 25 января 2018 г. № 189-О [2] и от 24 июня 2021 г. № 1364-О [1], конкретизируя процессуальный порядок доступа к цифровой коммуникации с учетом информационной емкости электронных устройств и облачной архитектуры мессенджеров. Ее нормативное закрепление усиливает гарантии частной жизни и доказательственную надежность цифровой информации за счет четкого определения проверяемого объема действий следователя.

Закключение

Исследование выявило системную несо-

гласованность между процессуальной формой действия и фактической интенсивностью вмешательства в частную жизнь. Исследование электронного устройства открывает доступ к значительному массиву частных коммуникаций, тогда как последующий судебный контроль в порядке ст. 125 УПК РФ не устраняет необратимость раскрытия сведений, не относящихся к предмету доказывания. Поэтому объем процессуальных гарантий должен зависеть от характера и интенсивности доступа к частной электронной коммуникации, а не от способа хранения или извлечения данных. Это выражает принцип функциональной эквивалентности вмешательства: сопоставимое ограничение конституционного права требует сопоставимого уровня процессуальной защиты.

Реализация этого принципа предполагает предварительное судебное разрешение на целевой доступ к цифровой переписке, определение предмета и временного интервала исследования, минимизацию избыточного ознакомления, техническую проверяемость действий, специальный режим неотложного доступа и последующее уведомление лица о фактическом объеме исследования. Для закрепления этих гарантий предлагается дополнить ст. 13 и ч.2 ст.29 УПК РФ, а также ввести ст. 186.2 УПК РФ «Получение и исследование сведений частных электронных коммуникаций». Технологически нейтральная конструкция позволяет использовать цифровую переписку в доказывании, обеспечивая определенность процедуры и судебную защиту частной жизни.

#### Список литературы:

[1] Определение Конституционного Суда Российской Федерации от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации»: документ опубликован не был [Электронный ресурс]. // Режим доступа: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=674396#RUZpqVVeys7geaKp1> (дата обращения: 20.09.2026).

[2] Определение Конституционного Суда Российской Федерации от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации»: документ опубликован не был [Электронный ресурс]. // Режим доступа: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=527893#tGOpqVVIRznV2991> (дата обращения: 20.09.2026).

[3] Алексеев К.А. Реализация конституци-

онного права на тайну переписки и переговоров в условиях развития цифровых технологий // Международный научно-исследовательский журнал. 2026. № 5 (167) [Электронный ресурс]. // Режим доступа: <https://research-journal.org/archive/5-167-2026-may/10.60797/IRJ.2026.167.47> (дата обращения: 20.09.2026).

[4] Зуев Д.И. Право на неприкосновенность частной жизни в современном уголовном процессе // Юридический вестник Самарского университета. 2024. Т. 10, № 4. С. 75-83.

[5] Иванов В.В. Защита охраняемых законом тайн при производстве следственных действий с мобильным телефоном и иными электронными носителями информации // Правовое государство: теория и практика. 2021. Т. 17, № 4 (66). С. 183-195.

[6] Недиков В.Б. Проблемы получения информации доказательственного значения по преступлениям, совершенным посредством использования социальных сетей и мессенджеров // Журнал юридических исследований. 2024. Т. 9, № 4. с. 122-128.

[7] Осипов А.Л. Защита права граждан на неприкосновенность их частных коммуникаций в уголовном судопроизводстве: национальный и зарубежный аспекты // Актуальные проблемы российского права. 2023. Т. 18, № 1 (146). С. 124-135.

[8] Сводные статистические сведения о деятельности федеральных судов общей юрисдикции и мировых судей за 1 полугодие 2025 года [Электронный ресурс]. // Режим доступа: <https://cdep.ru/index.php?id=79&item=9291> (дата обращения: 20.09.2026).

[9] Черкасов В.С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса: дис. ... канд. юрид. наук. Хабаровск, 2022. 210 с.

#### References:

[1] Determination of the Constitutional Court of the Russian Federation of 24.06.2021 No. 1364-O "On refusal to accept for consideration the complaint of citizen Fomin Evgeny Petrovich about violation of his constitutional rights by Articles 93, 176, 177 and part two of Article 184 of the Criminal Procedure Code of the Russian Federation": the document was not published [Electronic resource] //

Access mode: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=674396#RUZpqVVeys7geaKp1> (date of appeal: 20.09.2026).

[2] Determination of the Constitutional Court of the Russian Federation of 25.01.2018 No. 189-O "On refusal to accept for consideration the complaint of citizen Prozorovsky Dmitry Alexandrovich about violation of his constitutional rights by Articles 176, 177 and 195 of the Criminal Procedure Code of the Russian Federation": the document was not published [Electronic resource] // Access mode: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=527893#tGOpqVVIRzvnN2991> (date of appeal: 20.09.2026).

[3] Alekseev K.A. Realization of the constitutional right to secrecy of correspondence and negotiations in the context of the development of digital technologies // International Research Journal. 2026. No. 5 (167) [Electronic resource] // Access mode: <https://research-journal.org/archive/5-167-2026-may/10.60797/IRJ.2026.167.47> (access date: 20.09.2026).

[4] Zuev D.I. The right to privacy in modern criminal proceedings // Legal Bulletin of Samara University. 2024. VOL. 10, NO. 4. S. 75-83.

[5] Ivanov V.V. Protection of legally protected secrets in the conduct of investigative actions with a mobile phone and other electronic media // Rule of law: theory and practice. 2021. Т. 17, NO. 4 (66). S. 183-195.

[6] Nedikov V.B. Problems of obtaining information of evidentiary value on crimes committed through the use of social networks and instant messengers // Journal of Legal Research. 2024. Т. 9, NO. 4. from. 122-128.

[7] Osipov A.L. Protection of the right of citizens to inviolability of their private communications in criminal proceedings: national and foreign aspects // Current problems of Russian law. 2023. Т. 18, NO. 1 (146). S. 124-135.

[8] Summary statistics on the activities of federal courts of general jurisdiction and justices of the peace for the 1 half of 2025 [Electronic resource] // Access mode: <https://cdep.ru/index.php?id=79&item=9291> (date of appeal: 20.09.2026).

[9] Cherkasov V.S. Legal regulation of the use of electronic means in proving at the pre-trial stages of criminal proceedings: dis.... cand. jurid. sciences. Khabarovsk, 2022. 210 s.

