УДК 343.102

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ: ПРОБЛЕМА ПРАВОВОЙ ОПРЕДЕЛЕННОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ (СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ)

Владимир Юрьевич Жандров
Московский университет МВД России имени В. Я. Кикотя, Москва, Россия, vaisvladimir74@gmail.com

Аннотация. Использование криминалитетом преимуществ информационно-телекоммуникационных технологий требует адаптации методов оперативно-разыскной деятельности к новым условиям документирования. Нашедшее свое отражение в практике международно-правового регулирования электронное наблюдение становится перспективным инструментом противодействия киберпреступности, но при этом остается в состоянии правовой неопределенности в российском правовом поле. Этим определяется цель исследования — на основе анализа международно-правовых актов, зарубежного законодательства и практики его применения определить оптимальную модель формализации электронного наблюдения в российском праве.

Общую правовую основу обособления электронного наблюдения в качестве самостоятельной формы негласного контроля создают ратифицированные Россией международно-правовые акты и документы Организации Объединенных Наций. Их положениями допускается перехват информации путем использования технических средств, а также удаленный доступ к сведениям, хранящимся на электронных носителях.

При всем разнообразии подходов к правовому регулированию электронного наблюдения в США и странах Западной Европы (Великобритании, Германии и Франции) общим является его законодательная формализация в качестве самостоятельного метода расследования с подробно регламентированной процедурой применения, включающей судебный и институциональный контроль. Совершенствование оперативно-разыскной деятельности в условиях цифровизации может быть достигнуто путем нормативного закрепления электронного наблюдения в российском законодательстве, что позволит достичь сопоставимости с зарубежными практиками, укрепить правовые гарантии прав человека и упорядочить правоприменение при получении цифровых доказательств.

Ключевые слова: оперативно-разыскное мероприятие, методы оперативно-разыскной деятельности, киберпреступность, электронное наблюдение, цифровые доказательства, информационно-телекоммуникационные технологии

Для цитирования: Жандров В. Ю. Электронное наблюдение: проблема правовой определенности в условиях цифровизации оперативно-разыскной деятельности (сравнительное исследование) // Вестник Волгоградской академии МВД России. 2025. № 4 (75). С. 175—187.

ELECTRONIC SURVEILLANCE: THE PROBLEM OF LEGAL CERTAINTY IN THE CONTEXT OF DIGITALIZATION OF DETECTIVE ACTIVITIES (A COMPARATIVE STUDY)

Vladimir Yuriyevich Zhandrov
Kikot Moscow University of the Ministry of Internal Affairs of Russia, Moscow, Russia, vaisvladimir74@gmail.com

Abstract. To apply the advantages of information and telecommunications technologies by the criminal community requires the adaptation of detective methods to new documentation requirements. Electronic surveillance, being an element in the international legal regulation, is becoming a promising tool to counteract cyber-

crime, but remains in legal uncertainty conditions in the Russian legal context. This fact determines the purpose of this study based on an analysis of the international legal acts, foreign legislation, and its application. It means to identify the optimal model for formalizing electronic surveillance in Russian law.

General legal basis to identify electronic surveillance as an independent form of covert control is provided by international legal instruments and UN documents ratified by Russia. Their provisions permit the interception of information by using technical means, as well as remote access to information stored on electronic devices. Despite the diversity of approaches to the legal regulation of electronic surveillance in the United States and Western European countries (the United Kingdom, Germany, and France), the common thing is its legislative formalization as an independent investigative method with a detailed procedure for application, including judicial and institutional control. To improve detective activities in the context of digitalization can be achieved by normative fixation of electronic surveillance in Russian legislation. It makes possible to achieve comparability with international practices, strengthen legal guarantees of human rights, and streamline law enforcement while getting digital evidence.

Keywords: detective operations, detective methods, cybercrime, electronic surveillance, digital evidence, information and telecommunications technologies

For citation: Zhandrov V. Yu. Electronic surveillance: the problem of legal certainty in the context of digitalization of detective activities (a comparative study). Journal of the Volgograd Academy of the Ministry of the Interior of Russia, 175—187, 2025. (In Russ.).

Современный этап развития правовых систем и транснационального взаимодействия по вопросам обеспечения безопасности от криминальных угроз актуализирует поиск новых подходов, отвечающих наблюдаемой трансформации преступности в условиях развития информационно-телекоммуникационных технологий. Меняющиеся условия требуют от государств использования комплексных, технологически оснащенных и институционально встроенных подходов. Как справедливо отмечают Ю. А. Лапунова и А. Ю. Бегунов, «цифровое пространство является специфической средой осуществления ОРД, и ее ключевые элементы принципиально отличаются от осуществления ОРД в физической среде» [1, с. 259]. На этом фоне все более широкое признание получает так называемое электронное наблюдение — перспективный инструмент выявления и документирования преступной активности в информационно-телекоммуникационной среде, требующий теоретического обоснования и институционального признания в качестве самостоятельного метода оперативно-разыскной деятельности (далее — ОРД). Данная тенденция обусловлена не только технологической трансформацией коммуникационной среды, но и необходимостью выстраивания правовой определенности в применении скрытых средств цифрового контроля, на что обращалось внимание в литературе [2, с. 82].

Общую правовую основу легитимации электронного наблюдения создают *международно-правовые акты.* Так, в ст. 20 Конвенции Организации Объединенных Наций против транснациональной организованной преступности 2000 г.[1] и ст. 50 Конвенции против коррупции 2003 г.[2] указано на необходимость развития специальных методов расследования (англ. special investigative techniques), включая электронное наблюдение как самостоятельную форму скрытого контроля. Важным ориентиром для институционализации форм деятельности, основанных на цифровом контроле, имеют и положения разд. 34 «Электронное наблюдение» Модельного закона Организации Объединенных Наций о взаимной правовой помощи по уголовным делам (ред. 2022 г.)[3]. В документе прямо предусмотрена возможность использования электронных форм наблюдения в рамках международного сотрудничества, включая не только технический перехват информации, но и иные

[1] Конвенция Организации Объединенных Наций против транснациональной организованной преступности: принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml?ysclid=mcyv4joae0660309046 (дата обращения: 11.07.2025).

[2] Конвенция Организации Объединенных Наций против коррупции: принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml?ysclid=mcyv95nfxs855961268 (дата обращения: 11.07.2025).

[3] Модельный закон о взаимной правовой помощи по уголовным делам: подготовлен ООН (UNODC) на основе редакции 2007 г. с поправками 2022 г. // ООН: офиц. сайт. URL: https://www.unodc.org/documents/treaties/COP11/CRP/CTOC_COP_2022_CRP.4_E.pdf (дата обращения: 15.06.2025).

формы удаленного доступа, фиксации и хранения данных. В частности, упоминаются: организация трансграничного наблюдения за коммуникациями с согласия запрашиваемого государства; разрешение на использование программных средств для скрытого получения данных с устройств, расположенных на территории другого государства; возможность осуществления технического мониторинга в режиме реального времени; сохранение перехваченной информации в условиях, гарантирующих ее юридическую допустимость. И хотя какого-либо международного определения понятия «специальные методы расследования» не существует [3, с. 404], указанные положения подчеркивают, что электронное наблюдение рассматривается не как вспомогательный или сугубо национальный инструмент, а как признанная в международной практике форма оперативного реагирования на угрозы, исходящие из цифрового пространства.

Особенностью электронного наблюдения является высокая степень его технологической зависимости. Если классические методы опираются преимущественно на человеческий фактор, то последнее реализуется через взаимодействие с информационно-телекоммуникационными системами, предполагает использование инструментов киберразведки, анализ цифровых следов и обработку больших данных. Его методологическая специфика заключается в сочетании негласности, направленности на цифровую среду и способности формировать структурированный массив оперативной информации, обладающей потенциальной доказательственной ценностью.

Законное применение рассматриваемого метода допускается не только в фазе оперативного реагирования, но и на этапе уголовного преследования в качестве процессуально значимого средства уголовного судопроизводства. Таким образом, международная правовая практика наполняет электронное наблюдение достаточно обширным содержанием, охватывающим как доктринально-оперативный, так и процессуальный аспекты получения, фиксации и использования информации.

На уровне правового пространства регионального объединения государств — *Совета Европы* — электронное наблюдение также признается обособленным методом расследования. Ключевым межгосударственным актом, закрепляющим правовую основу для его применения, выступает Конвенция Совета Европы о киберпреступности (Будапештская конвенция, 2001 г.). В статьях 20 и 21 данного международного договора прямо указана допустимость сбора трафика и перехвата содержания информации в режиме реального времени. Эти положения институционализируют использование технических средств контроля как составной части законных мер расследования трансграничных преступлений, что объективно закрепляет статус электронного наблюдения как правомерного метода международного уголовного расследования[1].

По аналогии с общемировым уровнем правовая практика региональной организации государств Западной Европы относит электронное наблюдение к разновидности специальных методов расследования, используемых в условиях скрытности и повышенной сложности доказывания преступлений коррупционного и организованного характера. Согласно ст. 23 Конвенции об уголовной ответственности за коррупцию (заключена в г. Страсбурге 27 января 1999 г.)[2] и разъяснительному п. 114 к ней государствам-участникам предписывается принимать меры, способствующие сбору доказательств в условиях «пакта молчания» между преступниками. Среди таких мер перечисляются прослушивание телефонных разговоров, подслушивание, перехват телекоммуникаций, доступ к компьютерным системам и т. д.[3] И хотя термин «электронное наблюдение» напрямую в положениях международного договора не используется, указанные меры по своей сути составляют его технологическую и правовую основу. Подчеркивается, что использование перечисленных средств вмешательства требует строгого соблюдения принципов законности, соразмерности и подотчетности и должно сопровождаться правовыми и институциональными гарантиями, включая судебный контроль и национальное регулирование применения.

Аналогичная концепция прослеживается и в правовой системе *Европейского союза*, где электрон-

---

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). URL: https://rm.coe.int/1680081561 (дата обращения: 17.06.2025).

[2] Конвенция об уголовной ответственности за коррупцию (заключена в Страсбурге 27.01.1999). URL: https://www.consultant.ru/document/cons_doc_LAW_121544/5d2208398ec5fd926e0284b33f661990ddbf235c/ (дата обращения: 12.07.2025).

[3] Explanatory Report to the Criminal Law Convention on Corruption (ETS № 173). Strasbourg: Council of Europe, 1999. P. 28—29, § 114. URL: https://rm.coe.int/16800cce44 (дата обращения: 19.06.2025).

ное наблюдение интегрируется в более широкую категорию специальных методов расследования. В рамках многостороннего правового сотрудничества государств особое значение приобретает инициатива SIRIUS[1]. Проект представляет собой совместную инициативу Европола, Евроюста и Фронтекса (агентства Европейского союза (далее — ЕС), отвечающие за координацию и поддержку усилий стран — членов ЕС по охране внешних границ Шенгенской зоны), направленную на поддержку правоохранительных органов стран ЕС в вопросах получения цифровых доказательств от иностранных онлайн-сервисов (англ. Online Service Providers, OSPs), включая социальные сети, мессенджеры и облачные платформы, в условиях трансграничных расследований. SIRIUS обеспечивает развитие стандартов правового взаимодействия, консультативную и методическую поддержку, а также инструменты, облегчающие обращение к поставщикам цифровых данных в обход традиционных и часто длительных процедур.

Как следует из отчета Европола за 2019 г.[2], правоохранительные органы в первую очередь запрашивают регистрационную информацию, IP-адреса, метаданные, контент переписки и платежные сведения, т. е. именно те категории цифровых данных, которые традиционно ассоциируются с методами электронного наблюдения. Таким образом, практика, институционализированная через механизм SIRIUS, подтверждает легитимность и правоприменительную значимость электронного наблюдения как метода транснационального расследования.

Спецификой применения электронного наблюдения в правовом пространстве ЕС является подчиненность требованиям защиты персональных данных. В частности, положения Общего регламента по защите данных (GDPR)[3] и Директивы (ЕС) 2016/680[4], касающейся обработки персональных данных в правоохранительной сфере, формируют правовые рамки, в которых электронное наблюдение допускается как инструмент, находящийся под контролем закона и ограниченный требованиями защиты прав человека.

Так, в п. 49 GDPR прямо указывается, что государственные органы вправе осуществлять мониторинг и перехват коммуникаций для обеспечения сетевой и информационной безопасности, при условии соблюдения принципов строгой необходимости и пропорциональности. Эти же принципы получают развитие и в Директиве 2016/680, ст. 6 которой определяет законность обработки данных в целях предотвращения, расследования и пресечения преступлений, а ст. 10 устанавливает особые условия для работы с чувствительными категориями информации, допуская их использование только при наличии дополнительных правовых гарантий и в строго определенных целях.

Кроме того, пп. 4 и 71 GDPR устанавливают, что защита достоинства личности и ограничение автоматизированного вмешательства являются обязательными условиями, а профилирование допускается только при наличии законных оснований и соответствующих гарантий. Таким образом, вопреки отсутствию прямого указания на «электронное наблюдение», сущностные характеристики данного метода — скрытность, мониторинг, обработка цифровых следов и использование технических средств — институционализированы в праве ЕС как допустимые и значимые методы работы, применяемые исключительно в условиях надлежащего контроля и с учетом принципов демократического правопорядка.

Дополнительное развитие региональной позиции прослеживается в прецедентной практике *Европейского суда по правам человека* (далее — ЕСПЧ, Суд). Так, в решении по делу Klass and Others v. Germany (1978 г.) Суд впервые признал, что скрытое наблюдение за коммуникациями допустимо в демократическом обществе при наличии адекватных правовых гарантий и процедур контроля, обеспечивающих пропорциональность вмешательства целям правопорядка[5].

---

[1] SIRIUS — условное название проекта, используемое в официальных документах Европола.

[2] Europol. SIRIUS EU Digital Evidence Situation Report 2019. European Union Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu/publications-documents/sirius-eu-digital-evidence-situation-report-2019 (дата обращения: 17.06.2025).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Recital 49. URL: https://www.privacy-regulation.eu/en/recital-49-GDPR.htm (дата обращения: 17.06.2025).

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. Art. 6, 10. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj (дата обращения: 17.06.2025).

[5] Case of Klass and Others v. Germany, application № 5029/71, judgment of 6 September 1978 (Series A № 28) // European Court of Human Rights. § 48—50. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:%22001-57510%22}%20AND%20%22Paragraph48%22 (дата обращения: 17.06.2025).

В деле Liberty and Others v. the United Kingdom (2008) Суд пришел к выводу, что отсутствие в британском законодательстве четких и публичных правил, регулирующих перехват международных коммуникаций, нарушает ст. 8 Европейской конвенции, несмотря на формальное наличие санкционирующего механизма. Подчеркивается, что вмешательство в частную жизнь может быть правомерным лишь при наличии закона, который определенным образом ограничивает дискреционные полномочия властей, обеспечивает надлежащие процедурные гарантии и предоставляет возможность эффективного контроля[1]. Тем самым Суд институционализировал электронное наблюдение как правомерный метод только при условии, что оно регулируется детальной, доступной и предсказуемой правовой архитектурой.

В решении по иску Roman Zakharov v. Russia (2015 г.) ЕСПЧ указал, что государственная система массового перехвата нарушает ст. 8 Европейской конвенции, если она не сопровождается эффективными механизмами надзора, прозрачности и индивидуализированной авторизации. Однако при этом Суд подчеркнул: сам факт применения электронных методов наблюдения не противоречит международным правовым стандартам, если соблюдены требования законности, необходимости и пропорциональности вмешательства[2].

Таким образом, западноевропейская практика не отвергает электронное наблюдение, но оценивает его допустимость через призму правовой формы и процедурных гарантий. В этом контексте правовое признание метода складывается из трех взаимосвязанных компонентов: 1) наличия законодательного регулирования; 2) судебного или иного внешнего контроля; 3) средств обжалования или компенсации. В практике ЕСПЧ эти принципы выражены наилучшим образом, благодаря чему электронное наблюдение признается инструментом, совместимым с демократическими стандартами при условии наличия «достаточно точной и предсказуемой правовой базы».

Исследовательский интерес представляет опыт отдельных государств, закрепляющих электронное наблюдение как допустимый и юридически значимый метод в собственных правовых системах.

В **США** основополагающим актом, определяющим содержание и пределы электронного наблюдения, выступает Закон о наблюдении в целях внешней разведки[3] (Foreign Intelligence Surveillance Act of 1978[4], далее — FISA), который дает четкое определение понятию данного метода, требующего получения специального ордера FISC даже для целей национальной безопасности.

Уже само название закона концептуализирует электронное наблюдение как самостоятельный элемент разведывательной деятельности, отличающийся от разрозненных технических операций. В § 101 (f) FISA содержится развернутое и юридически значимое определение electronic surveillance, охватывающее четыре ключевых случая: 1) перехват содержания проводных или радиосообщений с использованием технических средств; 2) установка электронных устройств наблюдения в целях сбора информации о поведении лица в США, если от этого лица в обычной ситуации ожидалась бы конфиденциальность; 3) целенаправленное наблюдение за объектом с территории США без использования прямой прослушки, если в аналогичной ситуации потребовался бы ордер; 4) любые формы тайного сбора информации, подпадающие под

[1] Liberty and Others v. the United Kingdom, № 58243/00, Judgment of 1 July 2008 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-87207 (дата обращения: 18.06.2025).

[2] Case of Roman Zakharov v. Russia [GC], application № 47143/06, judgment of 4 December 2015 // European Court of Human Rights. § 227—234. URL: https://hudoc.echr.coe.int/eng?i=001-159324 (дата обращения: 17.06.2025).

[3] Официальное название акта — Foreign Intelligence Surveillance Act of 1978, что дословно переводится как «Закон о внешней разведке, осуществляемой посредством электронного наблюдения, 1978 года» или в кратком варианте — «Закон о наблюдении за иностранной разведкой». Однако юридически корректным и в то же время более точным переводом следует считать «Закон о наблюдении в целях внешней разведки». Это обусловлено тем, что сам закон регулирует проведение электронного наблюдения (electronic surveillance) внутри территории США для получения разведывательной информации о деятельности иностранных держав, их агентов и организаций. Он не только допускает перехват коммуникаций, но и описывает процедуры, полномочия, минимизацию ущерба для граждан США и систему судебного контроля (включая создание специального суда — FISA Court). В тексте закона это название формулируется в преамбуле: «This Act may be cited as the „Foreign Intelligence Surveillance Act of 1978“» (см.: Public Law 95-511—OCT. 25, 92 Stat. 1783. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (дата обращения: 12.07.2025)).

[4] Foreign Intelligence Surveillance Act of 1978. Public Law 95-511. Title I. URL: https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter36&edition=prelim (дата обращения: 19.06.2025).

действия первого, второго или третьего случая[1]. Таким образом, электронное наблюдение по FISA охватывает как перехват цифровых и аналоговых коммуникаций, так и визуальное наблюдение, техническое вторжение, сбор метаданных и прочих следов активности — при условии, что они осуществляются негласно в интересах национальной безопасности.

Закон требует обязательного судебного контроля за большинством форм электронного наблюдения. Согласно § 105 FISA санкция на его проведение выдается специальным Судом по надзору за внешней разведкой (англ. Foreign Intelligence Surveillance Court, FISC), который рассматривает обращения разведывательных и контрразведывательных органов на предмет их соответствия критериям необходимости, обоснованности и законности[2]. При этом § 111 FISA закрепляет обязанность Министерства юстиции США регулярно представлять отчетность Конгрессу о масштабах, содержании и результатах использования электронного наблюдения, что является гарантией институционального контроля над деятельностью спецслужб[3]. Следовательно, в системе права США электронное наблюдение рассматривается как комплексный, строго регламентированный метод разведывательной и правоохранительной деятельности, находящийся под контролем закона, суда и парламента.

Значительное развитие институциональных форм электронного наблюдения отмечается и в правовой системе **Великобритании**. Закон о полномочиях в сфере расследований 2016 г. (Investigatory Powers Act 2016[4], IPA) закрепляет возможность использования целенаправленного вмешательства в работу оборудования (англ. targeted equipment interference) и массового перехвата (англ. bulkinterception), легализуя как персонифицированные, так и тотальную формы цифрового контроля при условии соблюдения строгих процедур авторизации.

Закрепленное ч. 5 акта целенаправленное вмешательство в работу оборудования заключается в санкционированном скрытном вмешательстве в цифровые устройства (включая компьютеры, смартфоны и иные носители), позволяющее получать доступ к содержанию, метаданным и системной информации. Ордер на такие действия может быть выдан лишь при соблюдении условий законности, соразмерности и необходимости и требует утверждения уполномоченным судебным органом[5].

В частях 6.1—6.3 IPA регулируется практика массового сбора данных связи (англ. bulkacquisition of communications data) и вмешательство в работу оборудования (англ. bulkequipment interference) — масштабного, негласного сбора цифровых данных, включая перехват телекоммуникационного трафика, извлечение информации из облачных сервисов, сетевых хранилищ и локальных устройств. Такие формы наблюдения предназначены для целей национальной безопасности, предотвращения терроризма и тяжких преступлений[6]. Контроль за соблюдением процедур осуществляется в соответствии с ч. 7 закона, устанавливающей институциональные гарантии, включая должность Уполномоченного по вопросам наблюдательной деятельности (англ. Investigatory Powers Commissioner), а также механизмы правового пересмотра и отчетности перед парламентом[7].

В целом британская модель электронного наблюдения охватывает как индивидуализированные, так и массовые формы технического контроля, которые прямо институционализированы в правовой системе как методы, соотносимые с понятием специальных следственных действий.

Национальное право **Германии** демонстрируют различную степень формализации электронного наблюдения как самостоятельного метода.

[1] Foreign Intelligence Surveillance Act of 1978: Public Law 95-511. § 101(f) // United States Statutes at Large. Vol. 92. Washington: U.S. Government Publishing Office, 1978. P. 1785—1786. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (дата обращения: 17.06.2025).

[2] Foreign Intelligence Surveillance Act of 1978: Public Law 95-511. § 105 // United States Statutes at Large. Vol. 92. P. 1788—1790. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (дата обращения: 17.06.2025).

[3] Foreign Intelligence Surveillance Act of 1978: Public Law 95-511. § 111 // United States Statutes at Large. Vol. 92. P. 1791. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (дата обращения: 17.06.2025).

[4] Investigatory Powers Act 2016. UK Public General Acts. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (дата обращения: 19.06.2025).

[5] Investigatory Powers Act 2016. UK Public General Acts. Part 5, § 99—104. URL: https://www.legislation.gov.uk/ukpga/2016/25/part/5 (дата обращения: 17.06.2025).

[6] Ibid. Part 6, Chapters 1—3, § 119—190. URL: https://www.legislation.gov.uk/ukpga/2016/25/part/6 (дата обращения: 17.06.2025).

[7] Ibid. Part 7, § 196—229. URL: https://www.legislation.gov.uk/ukpga/2016/25/part/7(дата обращения: 17.06.2025).

Конкретно в § 100a Уголовно-процессуального кодекса страны (StPO) закреплено право следственных органов на перехват телекоммуникаций при наличии судебного решения, включая внедрение в ИТ-системы подозреваемых, что квалифицируется как «принудительное средство, применяемое в уголовном процессе» (нем. Zwangsmittel)[1] в рамках как процессуального, так и доследственного производства.

StPO прямо регулирует возможность негласного перехвата и записи телекоммуникаций по решению суда при расследовании тяжких преступлений. В тексте закона для обозначения такой меры используется термин Telekommunikationsüberwachung, который в германской юридической практике соответствует понятию электронного наблюдения. Он охватывает не только классический перехват коммуникаций без ведома участников, но и использование технических средств внедрения в информационные системы в целях извлечения незашифрованной информации. Закон допускает, что могут быть перехвачены и текущие телекоммуникации, и сведения, хранящиеся на устройствах обвиняемого, если они могли бы быть получены в момент передачи в публичной сети.

В § 100a StPO определен перечень преступлений, в отношении которых возможно применение наблюдения, и включает технические, правовые и организационные гарантии: от требований минимизации вмешательства до обязательной судебной санкции и защиты конфиденциальности.

Таким образом, в немецком уголовно-процессуальном праве электронное наблюдение закреплено как процессуально регламентированный и институционально признанный метод расследования, обладающий правовым статусом и встроенный в систему надзора и ответственности.

Французский Кодекс внутренней безопасности (франц. Code de la sécurité intérieure, CSI) предусматривает возможность доступа к данным связи, включая удаленный доступ к устройствам, при наличии соответствующего уведомления уполномоченного органа[2]. В такой форме электронное наблюдение прямо институционализировано как часть системы разведывательных и правоохранительных мер.

Закон различает административные меры, применяемые до возбуждения уголовного дела (в том числе в целях предотвращения террористических актов), и меры судебного характера, санкционируемые в рамках уголовного преследования. В частности, ст. L. 854-1—L.854-9 регулируют порядок проведения наблюдения за международными электронными коммуникациями, включая скрытый доступ к содержимому сообщений, метаданным, а также данным, передаваемым через трансграничные телекоммуникационные каналы. Эти действия допускаются при наличии санкции премьер-министра и последующего контроля со стороны независимого органа — Национальной комиссии по контролю за разведывательной деятельностью (CNCTR), а также подлежат возможному обжалованию в Государственный Совет (франц. Conseil d'État)[3].

Кроме того, ст. L. 232-1—232-2 позволяют органам внутренней безопасности обрабатывать и использовать данные телекоммуникационного трафика в целях предотвращения терроризма, что отражает интеграцию электронного наблюдения в стратегию обеспечения национальной безопасности[4]. В законе подчеркивается, что такие меры — не просто технические процедуры, а нормативно санкционированные методы сбора разведывательной информации. Следовательно, правовая традиция континентальной Европы, включая Францию, подтверждает тенденцию восприятия электронного наблюдения как институционально оформленного метода, применяемого в оперативно-разыскной и разведывательной деятельности.

Таким образом, в современной международной правовой парадигме электронное наблюдение воспринимается не просто как отдельный вспомогательный технический прием получения информации. Установленные правовые рамки формируют его как структурированный обладающий процедурной формализацией и нормативной определенностью метод, встроенный в институциональную систему правосудия и национальной безопасности. Он не конкурирует, а дополняет существующую систему, предоставляя правоохранительным органам инструменты работы в цифровой среде,

[1] Strafprozessordnung (StPO). § 100a. Telekommunikationsüberwachung. BGBl. I S. 581, zuletztgeändert 2023. URL: https://www.gesetze-im-internet.de/stpo/__100a.html (дата обращения: 19.06.2025).

[2] Code de la sécurité intérieure. Livre VIII, art. L. 851-1 — L. 853-1. URL: https://www.legifrance.gouv.fr/codes/id/LEGISCTA000027989748/ (дата обращения: 19.06.2025).

[3] Code de la sécurité intérieure. Art. L854-1 — L854-9 // Légifrance. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000032026434/ (дата обращения: 18.06.2025).

[4] Code de la sécurité intérieure. Art. L232-1—L232-2 // Légifrance. URL: https://www.legifrance.gouv.fr/codes/id/LEGISCTA000027895205 (дата обращения: 18.06.2025).

которая становится основным полем преступной активности XXI в.

Представленные в сравнительно-правовом анализе модели зарубежных государств демонстрируют разнообразие подходов к правовому признанию электронного наблюдения, однако объединяются в понимании необходимости его формализации, судебной обозримости и нормативной ограниченности. Международные договоры, судебная практика Европейского суда по правам человека, правовые позиции Совета Европы и ЕС, а также национальные законодательства таких государств, как США, Великобритания, Германия и Франция, последовательно не только закрепляют электронное наблюдение в качестве допустимого и правомерного инструмента технологического воздействия, но и рассматривают его как полноценный обладающий обособленной юридической значимостью метод оперативной и разведывательной деятельности.

Система международных и национальных стандартов направлена на обеспечение прозрачного, контролируемого и соразмерного применения электронного наблюдения, допустимости его использования на основе правовой регламентации и процедурной определенности. Особую значимость имеет тот факт, что электронное наблюдение не противопоставляется правам человека, а интерпретируется в качестве средства, допустимого при соблюдении принципа соразмерности вмешательства в частную жизнь и обеспечения эффективного контроля. Его нормативное оформление, судебная обозримость и институциональная интеграция позволяют утверждать, что оно стало неотъемлемой частью современной правовой архитектуры, способной обеспечивать как национальную, так и международную безопасность в условиях цифровой трансформации.

На фоне складывающегося мирового тренда следует признать — в отечественной теории до сих пор отсутствует формализованное признание электронного наблюдения как метода ОРД, что затрудняет решение задач противодействия киберпреступности. Как было показано выше, в международной модели электронное наблюдение охватывает весь комплекс действий — от сбора информации до ее использования в доказывании, что позволяет рассматривать его как полноценный, юридически значимый метод расследования, встроенный в систему процессуальных и институциональных гарантий. В российской же правовой системе оно преимущественно ограничивается стадией добывания сведений, предназначенных для последующей проверки в рамках уголовного дела, и воспринимается, главным образом, как совокупность технических приемов, применяемых в рамках ОРД, без придания ему статуса самостоятельного метода, применимого в уголовно-процессуальном контексте. Это объясняется особенностями отечественной модели разграничения ОРД и уголовного процесса, в рамках которой ОРД предшествует процессуальной стадии, а методы расследования нормативно не классифицируются как самостоятельная правовая категория. В результате электронное наблюдение в России остается методологически встроенным в категорию технических средств ОРД, без выраженного процессуального контекста. Такой подход создает определенный разрыв между российской и международной правовыми доктринами. Указанное различие требует дальнейшего теоретического осмысления и, возможно, законодательной адаптации в контексте гармонизации отечественного законодательства с международными стандартами.

В этой связи важным представляется теоретический анализ электронного наблюдения, позволяющий определить его сущностные черты и отграничить от иных форм оперативной деятельности.

Некоторые авторы специальные методы расследования, включая электронное наблюдение, рассматривают в смысловой идентичности и тождественной сопоставимости с оперативно-разыскными мероприятиями [4, с. 92; 5, с. 120; 6; 7]. Полагаем, такой подход не вполне отвечает теоретической основе для разграничения методов и мероприятий.

Электронное наблюдение представляет собой совокупность оперативно-разыскных действий, направленных на скрытное дистанционное наблюдение, фиксацию, перехват и анализ цифровой информации, циркулирующей в информационно-телекоммуникационной среде. Как метод ОРД оно отличается от отдельных оперативно-разыскных мероприятий (далее — ОРМ) тем, что предполагает более широкую, структурированную систему действий, интегрирующих в себе как наблюдательные, так и аналитические элементы. Такая совокупность тактических и технических приемов выходит за пределы одного ОРМ и охватывает их комплекс — от анализа открытых источников до взаимодействия с конфидентами, находящимися в виртуальной среде, и внедрения программных средств контроля. Метод электронного наблюдения реализуется не только осуществлением таких мероприятий, как наблюдение, снятие информации с технических каналов связи,

прослушивание телефонных переговоров, получение компьютерной информации, но и способностью выступать как надсистема, объединяющая и направляющая отдельные мероприятия в единую тактическую концепцию. В этом контексте разработка понятия электронного наблюдения как метода ОРД является не столько произвольным конструктом, сколько результатом объективного развития предмета и метода оперативной науки.

На сегодняшний день в российском правовом поле отсутствует прямое упоминание электронного наблюдения в качестве самостоятельного метода ОРД. В то же время накопление исследовательского материала и трансформационные процессы в системе подзаконных актов и правоприменительной практике демонстрируют устойчивую тенденцию к институционализации данного метода в качестве правомерного инструмента, обладающего как оперативной, так и потенциальной значимостью для получения доказательств в новых технологических условиях. Сложившаяся неопределенность ставит вопрос, должна ли правовая система России прямо признать электронное наблюдение в качестве метода ОРД, и при положительном ответе определить оптимальную для этого форму.

Полагаем, что институциональное оформление электронного наблюдения возможно в рамках трех базовых моделей, каждая из которых имеет как преимущества, так и правовые риски.

Первая модель — «законодательная». Предложение о целесообразности законодательного закрепления термина «электронное наблюдение» уже высказывалось в литературе [8]. Принятие данной модели предполагает внесение прямого дополнения в Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее — закон «Об ОРД»), утверждающего электронное наблюдение в качестве отдельного и правомерного средства сбора информации. Законодательное решение позволит нормативно закрепить правовую природу метода, его дефиницию, определить условия, цели и допустимые пределы применения. Рассматриваемая модель обеспечит высокий уровень правовой определенности и надлежащую степень соответствия принципам законности, правовой ясности и предсказуемости, установленным, в частности, в практике ЕСПЧ (дела Kruslin v. France[1], Huvig v. France[2] и Zakharov v. Russia[3]). Однако для реализации данной модели потребуется серьезная нормативная работа, включающая согласование с положениями Конституции Российской Федерации (принята всенародным голосованием 12 декабря 1993 г., с изм., одобренными в ходе общерос. голосования 01.07.2020), а также нормами Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 г. № 174-ФЗ и федеральными законами о защите персональных данных и связи.

Вторая модель — «подзаконная». Альтернативой законодательному регулированию может стать разработка и утверждение подзаконных нормативных актов — ведомственных инструкций, административных регламентов или положений, в которых электронное наблюдение будет описано как допустимая форма получения информации. Такой подход гибок и позволяет быстрее адаптироваться к технологическим изменениям. Вместе с тем, по сравнению с законодательной моделью, он обладает меньшей степенью правовой легитимности. В частности, формализация метода через подзаконные акты без надлежащего упоминания в законе «Об ОРД» может быть расценена как противоречащая принципу правовой определенности и создавать риски признания доказательств, полученных с помощью электронного наблюдения, недопустимыми в уголовном процессе. Кроме того, применение методов, затрагивающих права на тайну связи и неприкосновенность частной жизни, требует законодательного регулирования в силу положений ст. 23—25 Конституции РФ.

Третья модель — «судебная». Этот способ базируется на признании электронного наблюдения правомерным методом через формирование устойчивой судебной практики. Постепенное закрепление его допустимости и законности может происходить через постановления Верховного Суда РФ, обзоры судебной практики, а также закрепляться в тексте решений Конституционного Суда РФ, устанавливающих допустимые пределы вмешательства в частную жизнь. Примером подобной модели является развитие института оперативного эксперимента и результатов негласного аудио- и видеоконтроля, допустимость которых изначаль-

[1] Kruslin c. France, № 11801/85, judgment of 24 April 1990 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-62183 (дата обращения: 21.06.2025).

[2] Huvig v. France, № 11105/84, judgment of 24 April 1990 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-57627(дата обращения: 21.06.2025).

[3] Roman Zakharov v. Russia, № 47143/06, judgment of 4 December 2015 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-159324 (дата обращения: 21.06.2025).

но не была прямо прописана в законе. Тем не менее уязвимостью такого подхода станет сохранение правовой неопределенности, что может привести к противоречиям в правоприменительной практике, особенно в условиях отсутствия единых критериев допустимости электронного наблюдения в качестве источника доказательств.

Как видно, каждая из предложенных моделей институционализации электронного наблюдения сопряжена с рядом существенных правовых рисков, требующих специального внимания.

Прежде всего законодательное или подзаконное закрепление метода может вступить в потенциальное противоречие с положениями ст. 23 и 24 Конституции РФ, гарантирующими право на неприкосновенность частной жизни, личную и семейную тайну, а также тайну переписки, телефонных переговоров и иных сообщений. Эти положения имеют характер непосредственного действия и подлежат безусловному соблюдению со стороны всех органов государственной власти, включая правоохранительные структуры. Без надлежащих правовых гарантий такие вмешательства могут квалифицироваться как непропорциональные и произвольные, нарушающие базовые принципы конституционного правопорядка.

Отсутствие четко регламентированного механизма судебного контроля за проведением электронного наблюдения также остается одним из наиболее уязвимых элементов действующей системы. В свое время ЕСПЧ в упоминавшемся выше деле Zakharov v. Russia прямо указал на наличие «широких дискреционных полномочий правоохранительных органов» и недостаточную институциональную защищенность прав граждан, чьи коммуникации могут подвергаться перехвату. В этом решении Суд пришел к выводу, что система массового технического контроля в России на тот период не соответствовала требованиям «необходимости в демократическом обществе», поскольку не обеспечивала эффективного и независимого надзора, а применяемые меры носили чрезмерный характер по отношению к поставленным целям.

Наконец, с внедрением электронного наблюдения в качестве формализованного метода ОРД неизбежно возникнет вопрос о допустимости полученных с его помощью данных в уголовном процессе. Действующее законодательство в ст. 75 УПК РФ устанавливает для этого жесткие критерии и предусматривает запрет на использование доказательств, полученных с нарушением закона. Поскольку цифровые следы, получаемые в ходе электронного наблюдения, обладают особой технической спецификой (в том числе возможностью изменения, трудностью верификации источника и др.), для обеспечения их правовой значимости необходим пересмотр ряда процессуальных норм, а также внедрение дополнительных стандартов идентификации, фиксации и хранения такой информации.

В силу указанного институционализация электронного наблюдения потребует не только юридического признания, но и внедрения полноценной системы гарантий, способных обеспечить баланс между эффективностью правоохранительной деятельности и защитой конституционных прав личности.

С учетом проведенного анализа правовых подходов, действующих в ряде европейских государств и в Соединенных Штатах Америки, возможно выдвинуть ряд нормативных рекомендаций по включению электронного наблюдения в российское законодательство как самостоятельного метода ОРД.

Во-первых, следует нормативно закрепить понятие электронного наблюдения как отдельного метода, предполагающего скрытое или негласное получение, запись, хранение и анализ цифровой информации, передаваемой по каналам связи или хранящейся на электронных носителях. Такая дефиниция уже содержится, например, в американском Законе о наблюдении в целях внешней разведки (FISA), где термин electronic surveillance охватывает широкий спектр форм доступа к информации без ведома лица, включая удаленное вторжение в системы и перехват сообщений[1].

Во-вторых, правовая модель должна включать исчерпывающий перечень тяжких преступлений, при расследовании которых применение электронного наблюдения как метода ОРД допустимо. Аналогичный подход закреплен, в частности, в § 100a Уголовно-процессуального кодекса Германии (StPO), где телекоммуникационное наблюдение возможно лишь при наличии подозрения в совершении особо опасных деяний, включая терроризм, организованную преступность, коррупцию и тяжкие преступления против личности[2]. Такое

[1] Foreign Intelligence Surveillance Act of 1978. Public Law 95-511. Title I. § 101. URL: https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (дата обращения: 21.06.2025).

[2] Strafprozessordnung (StPO). § 100a Telekommunikationsüberwachung. BGBl. I S. 581, zuletztgeändert 2023. URL: https://www.gesetze-im-internet.de/stpo/__100a.html (дата обращения: 21.06.2025).

ограничение необходимо для обеспечения принципа пропорциональности вмешательства в частную жизнь.

В-третьих, обязательное судебное разрешение на проведение мероприятий по электронному наблюдению должно стать краеугольным камнем всей системы правовых гарантий. Без такой меры, как подчеркивается в практике Европейского суда по правам человека, невозможно обеспечить демократически допустимый уровень контроля над действиями правоохранительных органов[1].

В-четвертых, должна быть нормативно установлена процедура технической и юридической аутентификации полученных данных. Это предполагает не только криптографическую защиту, но и формализованные правила логирования, хеширования, хранения и представления цифровых следов, что позволяет гарантировать их допустимость и доказательственную силу в суде. Например, в изданном ЕС Руководстве по работе с цифровыми доказательствами для практиков подчеркивается важность строгого соблюдения процедурной непрерывности при обращении с электронными данными. В частности, указывается, что надлежащее документирование всех этапов доступа, хранения и анализа цифровой информации (англ. chain of custody) является необходимым условием ее допустимости в суде[2]. Это обусловлено тем, что цифровые доказательства, в силу своей нематериальной природы, подвержены риску несанкционированного изменения, потери или подделки. Таким образом, международные стандарты требуют от правоохранительных органов наличия технической инфраструктуры и правовых регламентов, обеспечивающих достоверность и воспроизводимость цифровой информации, полученной в ходе электронного наблюдения.

Наконец, в-пятых, необходимым элементом должна стать система институционального контроля за применением электронного наблюдения, включающая как внутриведомственные, так и независимые механизмы надзора, например в форме парламентских комиссий или уполномоченных комиссаров. Такая модель уже реализована в законодательстве Великобритании (Investigatory Powers Act 2016), предусматривающем работу Инспектората по надзору за полномочиями (Investigatory Powers Commissioner)[3].

Таким образом, институционализация электронного наблюдения обусловлена диалектической логикой научного анализа. Интеграция философского, правового и сравнительно-правового подходов позволяет сформировать теоретическую основу для признания его методом ОРД, обладающим всеми необходимыми для этого признаками (устойчивость, вариативность, тактическая самостоятельность, техническая обеспеченность) и ориентированного на цифровую среду как пространство оперативного интереса. В статусе метода ОРД электронное наблюдение требует комплексного нормативного и организационного оформления, соответствующего как требованиям национального конституционного порядка, так и международным стандартам в области прав человека и уголовного судопроизводства.

Разворачивающиеся в рамках российской криминальной ситуации новые криминальные угрозы объективно требуют включения данного метода в инструментарий, используемый для выявления, пресечения и расследования преступлений. Особенно остро данная проблема проявляется в цифровую эпоху, когда значительная часть юридически значимой информации формируется посредством скрытого доступа к электронным устройствам, цифровым сервисам и телекоммуникационным потокам. При отсутствии четкой правовой формы и процедурных рамок такой способ получения данных остается уязвимым с точки зрения допустимости в уголовном процессе и вызывает сомнения относительно его юридической устойчивости. Кроме того, в отсутствие прямого нормативного закрепления электронного наблюдения в качестве самостоятельного метода ОРД сохраняется состояние правовой неопределенности, которое затрудняет формирование последовательной следственно-судебной практики.

Для России наиболее эффективной представляется гибридная модель, сочетающая законодательное закрепление электронного наблюдения в законе «Об ОРД» с детальной регламентацией технических и процедурных аспектов в подзаконных актах, при обязательном условии установления независимого судебного и институционального контроля.

[1] Roman Zakharov v. Russia, № 47143/06, judgment of 4 December 2015.

[2] Manual on Digital Evidence for Practitioners — EU Judicial Cooperation. April 2019. P. 6—9. URL: https://www.ejn-crimjust.europa.eu/ejn/libcategories/EN/95/ (дата обращения: 19.06.2025).

[3] Investigatory Powers Act 2016 // UK Public General Acts. Part 8. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (дата обращения: 21.06.2025).

Признание электронного наблюдения методом ОРД должно базироваться не только на необходимости правового закрепления, но и на внутренней логике системного подхода к оперативной информации. Метод не сводится к контролю за информацией: он структурирует и объективирует сведения, формирует логически завершенные следы поведения субъекта, что принципиально отличает его от технических способов сбора данных. Электронное наблюдение требует соблюдения особых процедур верификации, аутентификации и фиксации, что делает его юридически значимым лишь при наличии соответствующего процессуального и ведомственного регламента. Только при соблюдении этих условий возможно признание электронного наблюдения в качестве полноценного метода ОРД, способного обеспечить оперативную эффективность, не нарушая при этом фундаментальные права личности.

Таким образом, институционализация электронного наблюдения не является факультативной задачей, но представляет собой необходимое условие процесса цифровизации ОРД. Формализация данного метода в законодательстве, включение его в нормативную систему Российской Федерации не просто допустимо, но и необходимо, поскольку будет способствовать укреплению правовых гарантий, упорядочиванию правоприменительной практики и формированию единой доктрины допустимости цифровых доказательств. При этом критически важным остается соблюдение условия его интеграции в систему гарантий, соразмерных уровню вмешательства в частную сферу, позволяющее выдержать баланс между публичным интересом обеспечения безопасности и защитой конституционных прав личности.

1. Лапунова Ю. А., Бегунов А. Ю. Полемика о концептуальных основах цифровой оперативно-розыскной деятельности // Оперативно-розыскная деятельность в цифровом мире: сб. науч. тр. / под ред. В. С. Овчинского. Москва: ИНФРА-М, 2021. С. 255—260.

2. Шаров В. И. Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. № 2 (64). С. 82—87.

3. Жданов Ю. Н., Овчинский В. С. Международное сотрудничество в борьбе с транснациональной организованной преступностью и терроризмом: специальные методы расследования, электронные доказательства, цифровые технологии // Оперативно-розыскная деятельность в цифровом мире: сб. науч. тр. / под ред. В. С. Овчинского. Москва: ИНФРА-М, 2021. С. 403—427.

4. Машковцев А. А., Моляров Е. А. Электронное наблюдение как современный способ оперативно-розыскного документирования преступлений // Вестник Сибирского юридического института МВД России. 2024. № 4 (57). С. 91—99.

5. Кольцов Д. В. Виды «специальных методов расследования» универсального уровня. Оперативно-розыскной взгляд // Труды Академии управления МВД России. 2023. № 4 (68). С. 118—130.

6. Соколов Ю. Н. Информационные технологии электронного наблюдения в расследовании преступлений // «Черные дыры» в российском законодательстве. 2010. № 1. С. 128—135.

1. Lapunova Yu. A., Begunov A. Yu. Discussion related to the conceptual foundations of digital detective activities. In: Detective activities in the digital world. Collection of scientific papers. Red. by V. S. Ovchinsky. Moscow: INFRA-M; 2021: 255—260. (In Russ.).

2. Sharov V. I. Detective activities on the Internet. Society and Law, 82—87, 2018. (In Russ.).

3. Zhdanov Yu. N., Ovchinsky V. S. International cooperation in the fight against transnational organized crime and terrorism: special investigative methods, electronic evidence, digital technologies. In: Detective activities in the digital world. Collection of scientific papers. Red. by V. S. Ovchinsky. Moscow: INFRA-M; 2021: 403—427. (In Russ.).

4. Mashkovtsev A. A., Molyarov E. A. Electronic surveillance as a modern method of detective documentation of crimes. 2021, 91—99, 2024. (In Russ.).

5. Koltsov D. V. Types of "special investigative techniques" at the universal level. Detective view. Works of the Academy of Management of the Ministry of the Interior of Russia, 118—130, 2023. (In Russ.).

6. Sokolov Yu. N. Information technologies of electronic surveillance in crime investigation. "Black holes" in Russian legislation, 128—135, 2010. (In Russ.).

7. Golubev V. V. Internet and detective activities. Legislation, 71—78, 1999. (In Russ.).

7. Голубев В. В. Интернет и оперативно-розыскная деятельность // Законодательство. 1999. № 11. С. 71—78.

8. Харевич Д. Л. О толковании термина «электронное наблюдение» в применении к Конвенции ООН против транснациональной организованной преступности // Юстиция Беларуси. 2010. № 4. С. 48—52.

8. Kharevich D. L. On the interpretation of the term "electronic surveillance" as applied to the UN Convention against Transnational Organized Crime. Justice of Belarus, 48—52, 2010. (In Russ.).

Жандров Владимир Юрьевич,
доцент кафедры
оперативно-разыскной деятельности
и специальной техники
Московского университета
МВД России имени В. Я. Кикотя,
кандидат юридических наук, доцент;
vaisvladimir74@gmail.com

Zhandrov Vladimir Yuriyevich,
associate professor at the department
of detective activities and special equipment
of the Kikot Moscow University
of the Ministry of Internal Affairs of Russia,
candidate of juridical sciences, docent;
vaisvladimir74@gmail.com

Статья поступила в редакцию 25.07.2025; одобрена после рецензирования 03.08.2025; принята к публикации 17.11.2025.

The article was submitted 25.07.2025; approved after reviewing 03.08.2025; accepted for publication 17.11.2025.

* * *